BB

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **11-261550**
(43)Date of publication of application : **24.09.1999**

(51)Int.CI. **H04L 9/32**
G06F 12/14
G06F 17/21
G09C 1/00

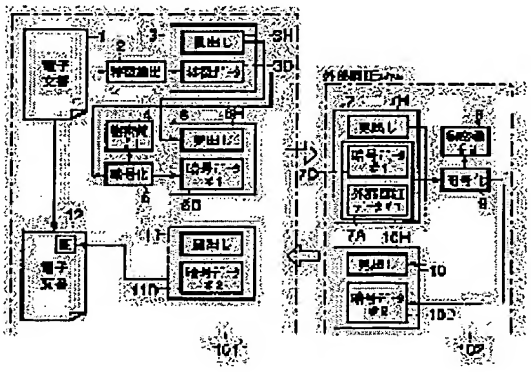
(21)Application number : **10-271541**
(22)Date of filing : **25.09.1998**

(71)Applicant : **TOSHIBA CORP**
(72)Inventor : **ONO KAZUTERU**

(30)Priority
Priority number : **10 717** Priority date : **06.01.1998** Priority country : **JP**

(54) SYSTEM AND METHOD FOR PREVENTING ELECTRONIC DOCUMENT FORGERY

(57)Abstract:
PROBLEM TO BE SOLVED: To add an evidence capability to an electronic document and also to promote document computerization in a true sense.
SOLUTION: This system is provided with a characteristics extracting means 11 which extracts a characteristics and produces characteristics data, a 1st enciphering means 5 which enciphers the characteristics data with the 1st key of cryptograph of the 1st person concerned and produces 1st enciphered data, a 2nd enciphering means 9 which adds external authentication data including at least a date to the 1st enciphered data enciphers it with the 2nd key of cryptograph of an external authenticating person and produces 2nd enciphered data, and a means which authenticates the 2nd enciphered data as authentication data of the electronic document.



LEGAL STATUS

[Date of request for examination] 05.03.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－261550

(43)公開日　平成11年(1999) 9月24日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５Ｂ
Ｇ０６Ｆ	12/14	３１０	Ｇ０６Ｆ	12/14	３１０Ｚ
	17/21		Ｇ０９Ｃ	1/00	６４０Ｂ
Ｇ０９Ｃ	1/00	６４０	Ｇ０６Ｆ	15/20	５７０Ｍ
			Ｈ０４Ｌ	9/00	６７３Ｄ

審査請求　未請求　請求項の数37　ＯＬ　（全 65 頁）　最終頁に続く

(21)出願番号　特願平10－271541

(22)出願日　平成10年(1998) 9月25日

(31)優先権主張番号　特願平10－717

(32)優先日　平10(1998) 1月6日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　小野　和輝
東京都府中市東芝町１番地　株式会社東芝府中工場内

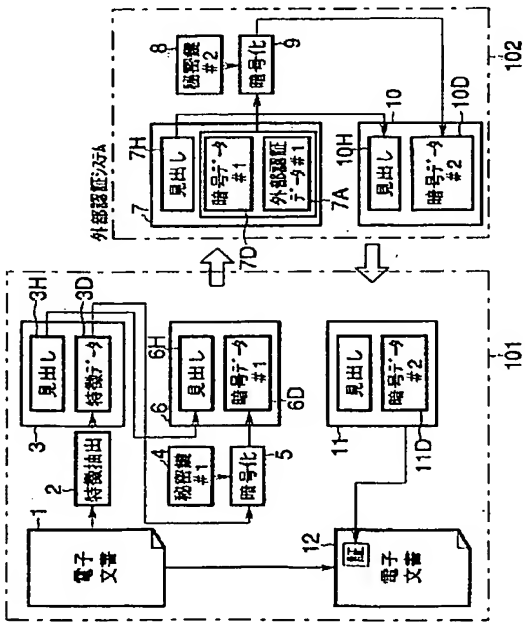
(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　電子文書の改竄防止システム及び方法

(57)【要約】

【課題】　本発明は、電子文書に証拠能力を付与するとともに、真の意味での文書の電子化を推進することを可能とする。

【解決手段】　電子文書から特徴を抽出して特徴データを生成する特徴抽出手段１１と、特徴データを第１の当事者の第１の暗号鍵で暗号化し、第１の暗号化データを生成する第１の暗号化手段５と、第１の暗号化データに、少なくとも日付を含む外部認証データを付加し、これを外部認証者の第２の暗号鍵で暗号化して第２の暗号化データを生成する第２の暗号化手段９と、第２の暗号化データを電子文書の認証データとする手段Ｓ１４とを備えた電子文書の改竄防止システム。



【特許請求の範囲】

【請求項１】　電子文書から特徴を抽出して特徴データを生成する特徴抽出手段と、
前記特徴データを第１の暗号鍵で暗号化して第１の暗号化データを生成する第１の暗号化手段と、
前記第１の暗号化データに、外部認証データを付加し、これを第２の暗号鍵で暗号化して第２の暗号化データを生成する第２の暗号化手段と、
前記第２の暗号化データを前記電子文書の認証データとする手段とを備える電子文書の改竄防止システム。

【請求項２】　電子文書から特徴を抽出して特徴データを生成する特徴抽出手段、前記特徴データを第１の暗号鍵で暗号化して第１の暗号化データを生成する第１の暗号化手段、前記第１の暗号化データを送信するとともに認証データを受信する第１の通信手段、および前記認証データを前記電子文書に対応させる手段とを備える文書認証システムと、
前記第１の通信手段にて送信される前記第１の暗号化データに、少なくとも日付を含む外部認証データを付加し、これを第２の暗号鍵で暗号化して第２の暗号化データを生成する第２の暗号化手段、および前記第１の暗号化データを受信するとともに前記第２の暗号化データを認証データとして前記文書認証システムに送信する第２の通信手段を備える外部認証システムと、を備えた電子文書の改竄防止システム。

【請求項３】　前記第１の暗号化データを第３の暗号鍵で暗号化して第３の暗号化データを生成する第３の暗号化手段を備え、前記第２の暗号化手段は、前記第１の暗号化データに代えて、前記第３の暗号化データに外部認証データを付加して第２の暗号鍵で暗号化して第２の暗号化データを生成することを特徴とする請求項１又は２記載の電子文書の改竄防止システム。

【請求項４】　前記第２の暗号化データを、前記第２の暗号鍵とは異なる第４の暗号鍵で暗号化して第４の暗号化データを生成し、前記認証データとする第４の暗号化手段をを備えることを特徴とする請求項１，２又は３記載の電子文書の改竄防止システム。

【請求項５】　認証対象の電子文書に対応する認証データから第２の暗号化データを取り出し、これを第２の暗号鍵に対応する第２の公開鍵で復号化する第２の復号化手段と、
前記第２の復号化手段により復号化されたデータから第１の暗号化データを取り出し、これを第１の暗号鍵に対応する第１の公開鍵で復号化する第１の復号化手段と、
前記電子文書から特徴を抽出して照会用特徴データを生成する特徴抽出手段と、
前記第１の復号化手段により復号化されたデータから特徴データを取り出し、前記照会用特徴データと照合する照合手段とを備えたことを特徴とする認証文書確認システム。

【請求項６】　請求項５において、前記第２の復号化手段により復号化されたデータから第３の暗号化データを取り出し、これを第３の暗号鍵に対応する第３の公開鍵で復号化する第３の復号化手段を設け、
前記第１の復号化手段は前記第３の復号化手段により復号化されたデータから第１の暗号化データを取り出し、これを第１の暗号鍵に対応する第１の公開鍵で復号化することを特徴とする認証文書確認システム。

【請求項７】　特徴抽出対象データを１単位づつ読み出して、読み出した値を順に規定の単位数だけ加算してなる合計値を順次並べて第１の合計値列とする第１列生成手段と、
この１単位づつ読み出した値に対して前記規定の単位数だけ隔てた関係となる１単位づつ読み出した値を加算し、この加算した値に対して前記関係となる１単位づつ読み出した値を加算し、この加算を繰り返し、合計加算回数として前記規定の単位数回の加算を行って得られる合計値を順次並べて第２の合計値列とする第２列生成手段と、
前記第１の合計値列及び前記第２の合計値列を特徴データとして出力する手段とを備えたことを特徴とする特徴抽出装置。

【請求項８】　前記第１の合計値列を１単位づつ読み出して、読み出した値を順に規定の単位数だけ加算してなる合計値を順次並べて第３の合計値列とする第３列生成手段と、
前記第２の合計値列を１単位づつ読み出して、読み出した値を順に規定の単位数だけ加算してなる合計値を順次並べて第４の合計値列とする第４列生成手段と、
前記第３の合計値列及び前記第４の合計値列を特徴データとして出力する手段とを備えたことを特徴とする請求項７記載の特徴抽出装置。

【請求項９】　指紋読取手段と、
前記指紋読取手段で読み取った指紋データから特徴抽出を行い指紋特徴データを生成する指紋特徴抽出手段と、
前記指紋特徴データ及びパスワードから暗号鍵を生成する暗号鍵生成手段と、
前記指紋特徴データ、パスワード及び乱数値から秘密鍵及び公開鍵を生成する秘密鍵公開鍵生成手段と、
前記暗号鍵で前記暗号鍵自身と前記秘密鍵をそれぞれ暗号化する暗号化手段と、
前記暗号化手段で暗号化したデータ、指紋データ及びパスワードを本人認証データとする手段とを備えたことを特徴とする本人認証データ生成システム。

【請求項１０】　前記請求項９に記載された本人認証データ生成システムで生成した前記本人認証データ中のパスワードと、入力されたパスワードとを照合するパスワード照合手段と、
指紋読取手段と、
両パスワードが一致した場合には、前記指紋読取手段で

指紋読み取りを行い、前記本人認証データ中の指紋データと、前記指紋読取手段にて読み取られた指紋データとを照合する指紋照合手段と、
指紋照合が一致した場合には、前記本人認証データ中の指紋データから特徴抽出を行い指紋特徴データを生成する指紋特徴抽出手段と、
前記指紋特徴抽出手段にて生成された指紋特徴データ及びパスワードから暗号鍵を生成する暗号鍵生成手段と、
この生成された暗号鍵により本人認証データ内の暗号化された暗号鍵を復号して、前記生成された暗号鍵と復号した暗号鍵とを照合する暗号鍵照合手段と、
暗号鍵照合が一致した場合には、この暗号鍵を用いて前記本人認証データ中の暗号化した秘密鍵を復号する秘密鍵復号手段とを備えた秘密鍵復号システム。
【請求項１１】　指紋読取手段と、
前記指紋読取手段から読み取られる指紋データの境界を検出する境界検出手段と、
前記境界検出手段により境界検出された指紋データをエンボス処理するエンボス手段と、
前記エンボス手段によりエンボス処理された指紋データを輪郭トレースする輪郭トレース手段とを備えたことを特徴とする指紋データ抽出装置。
【請求項１２】　前記請求項１１に記載された指紋データ抽出装置から抽出された指紋データから複数の矩形領域を取り出す領域取出手段と、
前記矩形領域のデータと予め登録した複数パターンとを比較し、何れかのパターンとマッチングするか否かを判定するパターンマッチング手段と、
マッチングしたパターンに対応する数値を数列として並べ、当該数列を指紋特徴データとする手段とを備えたことを特徴とする指紋特徴抽出装置。
【請求項１３】　電子文書から特徴を抽出して特徴データを生成する特徴抽出ステップと、
前記特徴データを第１の当事者の第１の暗号鍵で暗号化し、第１の暗号化データを生成する第１の暗号化ステップと、
前記第１の暗号化データに、少なくとも日付を含む外部認証データを付加し、これを外部認証者の第２の暗号鍵で暗号化して第２の暗号化データを生成する第２の暗号化ステップと、
前記第２の暗号化データを前記電子文書の認証データとするステップとを有することを特徴とする電子文書の改竄防止方法。
【請求項１４】　電子文書から抽出したデータを第１の暗号鍵で暗号化して第１の暗号化データを生成する文書認証システムと、受信データを第２の暗号鍵で暗号化して第２の暗号化データを生成する外部認証システムとが通信回線で接続される電子文書の改竄防止システムであって、
文書認証システムにて生成した前記第１の暗号化データを、前記通信回線を介して前記外部認証システムに送信し、
外部認証システムでは、受信した前記第１の暗号化データに、少なくとも日付を含む外部認証データを付加し、これを第２の暗号鍵で暗号化して第２の暗号化データを生成し、この第２の暗号化データを認証データとして前記文書認証システムに送信し、
文書認証システムでは、受信した前記第２の暗号化データを認証データとして前記電子文書に対応させることを特徴とする電子文書の改竄防止方法。
【請求項１５】　第１の文書認証システムにて、電子文書から抽出したデータを第１の暗号鍵で暗号化して第１の暗号化データを生成し、第２の文書認証システムに送信し、
第２の文書認証システムにて、前記第１の文書認証システムより送信された前記第１の暗号化データを第３の暗号鍵で暗号化して第３の暗号化データを生成し、外部認証システムに送信し、
外部認証システムにて、前記第２の文書認証システムより送信された前記第３の暗号化データに外部認証データを付加し、これを第２の暗号鍵で暗号化して第２の暗号化データを生成し、少なくとも前記第１の文書認証システムに送信し、
当該第１の文書認証システムにて、受信した前記第２の暗号化データを認証データとして前記電子文書に対応させることを特徴とする電子文書の改竄防止方法。
【請求項１６】　前記請求項１，２又は３記載の電子文書の改竄防止システムにて生成された前記認証データから前記第２の暗号化データを取出し、これを前記第２の秘密鍵に対応する第２の公開鍵で復号化する第２の復号化ステップと、
前記第２の復号化ステップにより復号化されたデータから前記第１の暗号化データを取出し、これを前記第１の秘密鍵に対応する第１の公開鍵で復号化する第１の復号化ステップと、
前記電子文書から特徴を抽出して照合用特徴データを生成する特徴抽出ステップと、
前記第１の復号化ステップにより復号化されたデータから前記特徴データを取出し、これを前記照合用特徴データと照合する照合ステップと、
前記照合ステップによる照合結果と、前記第２の復号化手段により復号化されたデータから取り出された前記外部認証データによって、外部認証者による認証の事実及び認証の日付を出力するステップとを有することを特徴とする認証文書確認方法。
【請求項１７】　電子文書から特徴を抽出して特徴データを生成する特徴抽出手段と、
前記特徴データを第１の当事者の第１の暗号鍵で暗号化し、第１の暗号化データを生成する第１の暗号化手段と、

前記第１の暗号化データに、少なくとも日付を含む外部認証データが付加され、これが外部認証者の第２の暗号鍵によって暗号化されてなる第２の暗号化データが入力されるとともに、この第２の暗号化データを前記電子文書の認証データとする手段として、コンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項１８】　前記請求項１，２又は３記載の電子文書の改竄防止システムにて生成された前記認証データから前記第２の暗号化データを取出し、これを前記第２の秘密鍵に対応する第２の公開鍵で復号化する第２の復号化手段と、

前記第２の復号化手段により復号化されたデータから前記第１の暗号化データを取出し、これを前記第１の秘密鍵に対応する第１の公開鍵で復号化する第１の復号化手段と、

前記電子文書から特徴を抽出して照合用特徴データを生成する特徴抽出手段と、

前記第１の復号化手段により復号化されたデータから前記特徴データを取出し、これを前記照合用特徴データと照合する照合手段と、

前記照合手段による照合結果と、前記第２の復号化手段により復号化されたデータから取り出された前記外部認証データによって、外部認証者による認証の事実及び認証の日付を出力する手段として、コンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項１９】　電子文書から特徴が抽出されて特徴データが生成され、

次に、前記特徴データが第１の当事者の第１の暗号鍵で暗号化され、第１の暗号化データが生成され、

次に、前記第１の暗号化データに、少なくとも日付を含む外部認証データが付加されて、これが外部認証者の第２の暗号鍵で暗号化して第２の暗号化データが生成され、

最終的に、前記第２の暗号化データからなる構造を有するデータが記録されたコンピュータ読み取り可能な記録媒体。

【請求項２０】　電子文書から特徴が抽出されて特徴データが生成され、

次に、前記特徴データが第１の当事者の第１の暗号鍵で暗号化され、第１の暗号化データが生成され、

次に、前記第１の暗号化データが第２の当事者の第３の暗号鍵で暗号化され、第３の暗号化データが生成され、

次に、前記第３の暗号化データに、少なくとも日付を含む外部認証データが付加されて、これが外部認証者の第２の暗号鍵で暗号化して第２の暗号化データが生成され、

最終的に、前記第２の暗号化データからなる構造を有するデータが記録されたコンピュータ読み取り可能な記録媒体。

【請求項２１】　認証付き電子文書から電子文書を取り出して、これに変更を加えて、新たな電子文書を生成する文書変更手段と、

前記認証付き電子文書から取り出された元の電子文書と前記新たな電子文書との変更点を抽出して変更箇所データを取得する差分抽出手段と、

前記変更箇所データと前記新たな電子文書とをそれぞれ変更者認証する変更者認証手段と、

前記変更者認証手段により認証された各データを外部の認証システムに送出するとともに、それぞれを外部認証された認証データを受け取って、受け取った各認証データ及び前記新たな電子文書に基づいて、認証付き変更箇所データと新たな認証付き電子文書を生成する認証手段とを備えたことを特徴とする電子文書の改竄防止システム。

【請求項２２】　前記変更者認証手段は、

前記変更箇所データ及び又は前記新たな電子文書から特徴抽出して特徴データを出力する特徴抽出手段と、

前記特徴データを、前記新たな電子文書を生成した変更者の暗号化鍵で暗号化して出力する暗号化手段とを備えたことを特徴とする請求項２１記載の電子文書の改竄防止システム。

【請求項２３】　前記変更者認証手段は、

前記暗号化手段から出力されかつ前記新たな電子文書に対応する暗号化特徴データと、元の認証付き電子文書から取り出された以前の認証データとを結合して出力する結合手段を備えたことを特徴とする請求項２２記載の電子文書の改竄防止システム。

【請求項２４】　前記変更者認証手段は、

前記特徴抽出手段により特徴抽出された特徴データと、元の認証付き電子文書から取り出された以前の認証データとを結合して出力する結合手段を備え、

前記暗号化手段の暗号化対象として、前記結合手段からの出力データを前記特徴データに代えて入力することを特徴とする請求項２２記載の電子文書の改竄防止システム。

【請求項２５】　前記請求項２１乃至２４のうち何れか１項に記載された認証手段により生成された認証付き変更箇所データと認証付き電子文書とを含む変更済電子文書から、前記認証付き変更箇所データ及び前記認証付き電子文書を取り出す分離手段と、

前記請求項２１乃至２４のうち何れか１項に記載された文書変更手段、差分抽出手段、変更者認証手段及び認証手段と、

前記認証手段により生成された新たな認証付き変更箇所データ及び新たな認証付き電子文書と、前記分離手段で分離された元の認証付き変更箇所データとに基づき、新たな変更済電子文書を生成する結合手段とを備えたことを特徴とする電子文書の改竄防止システム。

【請求項２６】　前記請求項２１乃至２４のうち何れか１項に記載された前記変更者認証手段により認証された各データを受け取る受入手段と、
前記各データそれぞれに、少なくとも日付データ及び認証実行識別情報を結合する結合手段と、
この結合手段により結合された各データを外部認証機関の暗号鍵によって暗号化して、外部認証された認証データを作成する暗号化手段とを備えたことを特徴とする電子文書の外部認証システム。
【請求項２７】　前記請求項２６に記載の外部認証システムにより外部認証された認証データを、外部認証機関の復号鍵で復号する復号化手段と、
前記復号化手段により復号された認証データから、前記日付データ及び前記認証実行識別情報を取り出すデータ取出手段とを備えたことを特徴とする認証文書確認システム。
【請求項２８】　前記請求項２６に記載の外部認証システムにより外部認証された認証データが前記請求項２３に対応しかつ電子文書に対応するものである場合に、
前記復号化手段により復号された認証データから、前記以前の認証データを取り出す認証データ取出手段を備えたことを特徴とする請求項２７記載の認証文書確認システム。
【請求項２９】　前記復号化手段により復号された認証データのうち、前記請求項２２の暗号化手段で暗号化された暗号データが入力されるとともに、当該暗号データを変更者の復号鍵で復号して特徴データを取り出す第２の復号化手段と、
前記請求項２１の文書変更手段で得られた新たな電子文書から特徴抽出して比較用特徴データを出力する特徴抽出手段と、
前記第２の復号化手段で得られた特徴データと、前記特徴抽出手段で得られた比較用特徴データとを比較する照合手段とを備えたことを特徴とする請求項２８記載の認証文書確認システム。
【請求項３０】　前記請求項２６に記載の外部認証システムにより外部認証された認証データが前記請求項２４に対応しかつ電子文書に対応するものである場合に、
前記復号化手段により復号された認証データを変更者の復号鍵で復号する第２の復号化手段と、
前記第２の復号化手段で復号化された認証データから、前記以前の認証データを取り出す認証データ取出手段とを備えたことを特徴とする請求項２７記載の認証文書確認システム。
【請求項３１】　前記第２の復号化手段で復号化された認証データから、特徴データを取り出す分離手段と、
前記請求項２１の文書変更手段で得られた新たな電子文書から特徴抽出して比較用特徴データを出力する特徴抽出手段と、
前記分離手段で得られた特徴データと、前記特徴抽出手段で得られた比較用特徴データとを比較する照合手段とを備えたことを特徴とする請求項３０記載の認証文書確認システム。
【請求項３２】　前記請求項２６に記載の外部認証システムにより外部認証された認証データが前記請求項２２に対応しかつ前記変更箇所データに対応するものである場合に、
前記復号化された認証データのうち、前記請求項２２の暗号化手段で暗号化された暗号データが入力されるとともに、当該暗号データを変更者の復号鍵で復号して特徴データを取り出す第２の復号化手段と、
前記請求項２１の差分抽出手段で得られた変更箇所データから特徴抽出して比較用特徴データを出力する特徴抽出手段と、
前記第２の復号化手段で得られた特徴データと、前記特徴抽出手段で得られた比較用特徴データとを比較する照合手段とを備えたことを特徴とする請求項２７記載の認証文書確認システム。
【請求項３３】　前記請求項２５に記載された電子文書の改竄防止システムにより作成された変更済電子文書の変更部分についての認証確認を行うシステムであって、
前記請求項２８又は３０の認証文書確認システムと、前記請求項３２の認証文書確認システムとを備えるとともに、
複数回の変更を受けた最終的な変更済電子文書における認証付き電子文書から、最終変更回に関する認証データを取り出し、まずこれを前記請求項２６に記載の外部認証システムにより外部認証された認証データとして前記請求項２８又は３０の認証文書確認システムに入力し、
最終変更回以外の各回については、前記請求項２８又は３０の認証文書確認システムから出力される前記以前の認証データを、前記請求項２６に記載の外部認証システムにより外部認証された認証データとして、順次、前記請求項２８又は３０の認証文書確認システムに入力し、
また、複数回の変更を受けた最終的な変更済電子文書から、各回の認証付き変更箇所データを取り出し、この認証付き変更箇所データを変更箇所データ及び前記請求項２６に記載の外部認証システムにより外部認証された認証データに分離して、前記請求項３２の認証文書確認システムに入力し、
前記請求項２８又は３０の認証文書確認システムから得られた日付データ及び認証実行識別情報と、前記請求項３２の認証文書確認システムから得られた日付データ及び認証実行識別情報とを各変更回毎に照合することを特徴とする変更済電子文書の認証確認システム。
【請求項３４】　前記請求項２９又は３１の認証文書確認システムを備えるとともに、
最終的な変更済電子文書に包含される認証付き電子文書から取り出された認証データ及び新たな電子文書を、前記請求項２８又は３０の認証文書確認システムに代えて

前記請求項２９又は３１の認証文書確認システムに入力することを特徴とする請求項３３記載の変更済電子文書の認証確認システム。

【請求項３５】　認証付き電子文書から電子文書を取り出して、これに変更を加えて、新たな電子文書を生成する文書変更手段と、

前記認証付き電子文書から取り出された元の電子文書と前記新たな電子文書との変更点を抽出して変更箇所データを取得する差分抽出手段と、

前記変更箇所データと前記新たな電子文書とをそれぞれ変更者認証する変更者認証手段と、

前記変更者認証手段により認証された各データを外部の認証システムに送出するとともに、それぞれを外部認証された認証データを受け取って、受け取った各認証データ及び前記新たな電子文書に基づいて、認証付き変更箇所データと新たな認証付き電子文書を生成する認証手段として、コンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項３６】　前記変更者認証手段は、

前記変更箇所データ及び又は前記新たな電子文書から特徴抽出して特徴データを出力する特徴抽出手段と、

前記特徴データを、前記新たな電子文書を生成した変更者の暗号化鍵で暗号化して出力する暗号化手段として、コンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な請求項３５記載の記録媒体。

【請求項３７】　前記請求項２６に記載の外部認証システムにより外部認証された認証データを、外部認証機関の復号鍵で復号する復号化手段と、

前記復号化手段により復号された認証データから、前記日付データ及び前記認証実行識別情報を取り出すデータ取出手段として、コンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明はデータや文書等の電子文書の改竄を防止し、特に電子文書の証拠能力を確保する部分に特徴のある電子文書の改竄防止システム及び方法に関するものである。

【０００２】

【従来の技術】従来から取引記録、品質記録あるいは契約書等の文書は、文書改竄の疑惑を防止する為に、黒インクやボールペン等を用いて紙上に記入し署名や捺印を行っている。

【０００３】このように紙にインクで記載したものは、後に記載内容や日付を改竄しようとしても容易には改竄できない。紙は古くなると質が変化する為に、新しく偽の文書を作成しても判別が可能である。こうした紙とインクの特徴の為に、従来から重要文書は全て紙で保管されている。

【０００４】最近、電子署名技術が開発され、文書を作成した本人を証明する事ができるようになっている。この電子署名を説明する。

【０００５】図５３は電子文書に署名してその同一性を判定する従来の方法を示す図である。

【０００６】同図に示すように、まず、電子文書２０１ａから特徴抽出手段２０２で特徴データ２０３Ｄを取り出す。次に、この特徴データ２０３Ｄを秘密鍵２０４を用い、暗号化手段２０５により暗号化して暗号データ２０６Ｄを作成する。そして、この暗号データ２０６Ｄを元の電子文書２０１ａと一緒にして署名済み電子文書２０１ｂとして受取人に送信する。

【０００７】受取人は、受け取った電子文書２０１ｂ’から暗号データ２０６Ｄを取り出して送信者の公開鍵２１６を使用し復号化手段２１７により特徴データ２１８Ｄを取り出す。一方、電子文書２０１ｂ’から元の電子文書２０１ａに相当する電子文書２０１ａ’を取り出し、さらに特徴抽出手段２２０により特徴データ２２１を取り出す。特徴データ２２１を先の特徴データ２１８Ｄと照合手段２２により照合し本人の電子文書に相違無い事を確認する。

【０００８】このような電子文書であれば、その文書作成者は間違いなく本人である事を確認できる。しかし、作成者本人であれば、作成済みの文書を自由に改変することが可能である。したがって、作成者本人が、例えばコンピュータの日付を故意にずらせて文書の作成日付を護魔化す等の問題を生じ得る。

【０００９】ここで、特願平5-303773号公報に記載される「電子化文書処理システムおよびディジタル署名の生成方法」では、作成した文書に別の作者が一部変更を加えて、新しい文書にする時の認証方法が開示されている。

【００１０】しかし、作成した電子文書を、作成に関わった作者等以外の利害の対立する者に対して証拠書類として使用することは、作成に関わった作者等が共謀して改竄を行なえば証拠改竄が可能となることから適切とはいえない。すなわち特願平5-303773号公報の方法は、文書を証拠書類として電子化させることには馴染まず、社内文書を社内で使用する場合に限った電子化といえる。

【００１１】例えば製品の製造工程に従って、工程毎の担当者が、自分の担当工程に署名捺印を行なう組み立て記録等には適用できず、紙での運用となっている。また、定期検査の記録で、記録シートに数行の点検結果を追記して署名捺印を行なう場合にも、紙での運用になっていた。この様な物は製品安全の事故に対して、検査記録を証拠とする必要があり、共謀すれば改竄できる電子文書では証拠とはなり得なかった為である。

【００１２】

【発明が解決しようとする課題】このように文書作成者

本人は文書改竄を行う事ができるので、取引記録、品質記録あるいは契約書等の電子文書を本人が改竄していないことが証明できない。このため、現状のシステムでは電子文書に対する信用性は低く、重要書類は相変わらず紙で取り扱われている。

【００１３】しかし、紙の文書は保管に多くの場所を必要とし、必要な文書を取り出すのに時間が掛かる。また、遠方に送る時に本紙と同じ証拠能力を持つ必要が有る場合には、本紙を送る以外に方法が無い問題がある。

【００１４】一方、最近のコンピュータの発達で文書がワープロなどで作成される様になると、紙の形で保管しておくよりも、電子文書として保管する方が便利である。たとえば保管場所を取らない、必要な文書の検索が容易である等の利点を有する為であり、このため文書の電子化が社会一般的に進んで来ている。

【００１５】しかし、上記したように電子文書の証拠能力が不足している事から、重要文書の電子化ができず、たとえ電子化しても、証拠能力を有する紙文書が本紙として別途必要である。このため、重要文書に関しての保管場所が必要である等の問題は依然として解決されない。

【００１６】本発明は、このような実情を考慮してなされたもので、本来紙文書の特徴である証拠能力を電子文書に付与するとともに、真の意味での文書の電子化を推進することを可能とし、ひいては、文書の保管場所の削減、文書の検索の効率化、本紙の文書の遠方への即時配達等を実現できる電子文書の改竄防止システム及び方法を提供することを目的とする。

【００１７】また、本発明の他の目的は、複数人が複数時期に渡って一つの電子文書を作成する場合でも、変更文書を関係者全員で再承認する必要をなくしかつ文書改竄を防止して、紙文書の証拠能力以上の証拠能力を有する電子文書を作成可能とした電子文書の改竄防止システム及び方法を提供することにある。

【００１８】

【課題を解決するための手段】本発明の骨子は、電子文書から抽出された特徴データを第１当事者の暗号鍵で暗号化し、さらにこの暗号化された特徴データを外部認証者の暗号鍵で暗号化してその結果得られた暗号データを電子文書の認証データとして用いるところにある。

【００１９】このようにして得られる認証データは、他人によって改竄することはできないし、暗号化された特徴データを渡された悪意の外部認証者によっても改竄できない。つまり特徴データ自体に第１当事者の暗号がかけれているため、外部認証者がこれを改竄すれば電子文書が正当でないことが検出されるものである。さらに、一度外部認証された認証データは、外部認証者による暗号化のために、第１当事者本人によっても改竄することが不能となる。

【００２０】一方、もとの電子文書を改竄した場合には、改竄電子文書からの特徴データと、認証データに含まれる特徴データとの比較により、その改竄の事実が検出される。

【００２１】このように、本発明では、悪意の他人による場合はもちろんのこと、悪意の第１当事者、さらには悪意の外部認証者のいずれによる場合であっても、もし電子文書又は認証データが何れの段階で改竄されれば、どの段階で改竄が行われた場合であってもその改竄事実が検出される。

【００２２】また、上記課題の解決は、より具体的には、以下のような解決手段により実現される。

【００２３】まず、請求項１に対応する発明は、電子文書から特徴を抽出して特徴データを生成する特徴抽出手段と、特徴データを第１の暗号鍵で暗号化して第１の暗号化データを生成する第１の暗号化手段と、第１の暗号化データに、外部認証データを付加し、これを第２の暗号鍵で暗号化して第２の暗号化データを生成する第２の暗号化手段と、第２の暗号化データを電子文書の認証データとする手段とを備える電子文書の改竄防止システムである。

【００２４】本発明はこのような手段を設けたので、本来紙文書の特徴である証拠能力を電子文書に付与するとともに、真の意味での文書の電子化を推進することを可能とし、ひいては、文書の保管場所の削減、文書の検索の効率化、本紙の文書の遠方への即時配達等を実現することができる。

【００２５】次に、請求項２に対応する発明は、電子文書から特徴を抽出して特徴データを生成する特徴抽出手段、特徴データを第１の暗号鍵で暗号化して第１の暗号化データを生成する第１の暗号化手段、第１の暗号化データを送信するとともに認証データを受信する第１の通信手段、および認証データを電子文書に対応させる手段とを備える文書認証システムと、第１の通信手段にて送信される第１の暗号化データに、少なくとも日付を含む外部認証データを付加し、これを第２の暗号鍵で暗号化して第２の暗号化データを生成する第２の暗号化手段、および第１の暗号化データを受信するとともに第２の暗号化データを認証データとして文書認証システムに送信する第２の通信手段を備える外部認証システムと、を備えた電子文書の改竄防止システムである。

【００２６】本発明はこのような手段を設けたので、請求項１の発明と同様な効果が得られる他、通信回線を用いることで、第１の当事者と外部認証者と間で認証データ作成作業を便利かつ短時間に進めることができる。

【００２７】次に、請求項３に対応する発明は、請求項１又は２に対応する発明において、第１の暗号化データを第３の暗号鍵で暗号化して第３の暗号化データを生成する第３の暗号化手段を備え、第２の暗号化手段は、第１の暗号化データに代えて、第３の暗号化データに外部認証データを付加して第２の暗号鍵で暗号化して第２の

暗号化データを生成する電子文書の改竄防止システムである。

【００２８】本発明はこのような手段を設けたので、請求項１の発明と同様な効果が得られる他、認証データに第２の当事者の暗号鍵による暗号化を加え、この電子文書を第１の当事者、第２の当事者及び外部認証者の三者の認証になる電子傾斜区処とすることができる。

【００２９】次に、請求項４に対応する発明は、請求項１～３に対応する発明において、第２の暗号化データを、第２の暗号鍵とは異なる第４の暗号鍵で暗号化して第４の暗号化データを生成し、認証データとする第４の暗号化手段をを備える電子文書の改竄防止システムである。

【００３０】本発明はこのような手段を設けたので、例えば認証データ作成から長期間をへて、技術の進歩でその暗号が解読される可能性が生じたような場合でも、請求項１～３のうち何れか１項記載の電子文書の改竄防止システムにて生成された第２の暗号化データについて、再度の暗号化による外部認証者の再認証を行うことができ、電子文書の改竄に対する防御性を維持することができる。

【００３１】次に、請求項５に対応する発明は、認証対象の電子文書に対応する認証データから第２の暗号化データを取り出し、これを第２の暗号鍵に対応する第２の公開鍵で復号化する第２の復号化手段と、第２の復号化手段により復号化されたデータから第１の暗号化データを取り出し、これを第１の暗号鍵に対応する第１の公開鍵で復号化する第１の復号化手段と、電子文書から特徴を抽出して照会用特徴データを生成する特徴抽出手段と、第１の復号化手段により復号化されたデータから特徴データを取り出し、照会用特徴データと照合する照合手段とを備えた認証文書確認システムである。

【００３２】本発明はこのような手段を設けたので、本来紙文書の特徴である証拠能力が付与された電子文書について、その認証事実及び認証日を確認するとともに、真の意味での文書の電子化を推進するのに貢献できるシステムを提供することができる。これにより、ひいては、文書の保管場所の削減、文書の検索の効率化、本紙の文書の遠方への即時配達等を実現することができる。

【００３３】次に、請求項６に対応する発明は、請求項５に対応する発明において、第２の復号化手段により復号化されたデータから第３の暗号化データを取り出し、これを第３の暗号鍵に対応する第３の公開鍵で復号化する第３の復号化手段を設け、第１の復号化手段は第３の復号化手段により復号化されたデータから第１の暗号化データを取り出し、これを第１の暗号鍵に対応する第１の公開鍵で復号化する認証文書確認システムである。

【００３４】本発明はこのような手段を設けたので、第２の当事者を交えた電子契約書についても、請求項５の発明と同様な効果を得ることができる。

【００３５】次に、請求項７に対応する発明は、特徴抽出対象データを１単位づつ読み出して、読み出した値を順に規定の単位数だけ加算してなる合計値を順次並べて第１の合計値列とする第１列生成手段と、この１単位づつ読み出した値に対して規定の単位数だけ隔てた関係となる１単位づつ読み出した値を加算し、この加算した値に対して関係となる１単位づつ読み出した値を加算し、この加算を繰り返し、合計加算回数として規定の単位数回の加算を行って得られる合計値を順次並べて第２の合計値列とする第２列生成手段と、第１の合計値列及び第２の合計値列を特徴データとして出力する手段とを備えた特徴抽出装置である。

【００３６】本発明はこのような手段を設けたので、こうして得られた特徴データのみからではもとの電子文書を再現できず、その改変を行えばその旨を検出でき、かつ、もとの電子文書を大幅にデータ圧縮した特徴データを生成することができる。

【００３７】次に、請求項８に対応する発明は、請求項７に対応する発明において、第１の合計値列を１単位づつ読み出して、読み出した値を順に規定の単位数だけ加算してなる合計値を順次並べて第３の合計値列とする第３列生成手段と、第２の合計値列を１単位づつ読み出して、読み出した値を順に規定の単位数だけ加算してなる合計値を順次並べて第４の合計値列とする第４列生成手段と、第３の合計値列及び第４の合計値列を特徴データとして出力する手段とを備えた特徴抽出装置である。

【００３８】本発明はこのような手段を設けたので、請求項７の発明と同様な効果が得られる他、特徴データをより圧縮することができる。

【００３９】次に、請求項９に対応する発明は、指紋読取手段と、指紋読取手段で読み取った指紋データから特徴抽出を行い指紋特徴データを生成する指紋特徴抽出手段と、指紋特徴データ及びパスワードから暗号鍵を生成する暗号鍵生成手段と、指紋特徴データ、パスワード及び乱数値から秘密鍵及び公開鍵を生成する秘密鍵公開鍵生成手段と、暗号鍵で暗号鍵自身と秘密鍵をそれぞれ暗号化する暗号化手段と、暗号化手段で暗号化したデータ、指紋データ及びパスワードを本人認証データとする手段とを備えた本人認証データ生成システムである。

【００４０】本発明はこのような手段を設けたので、指紋等を用いて有効な本人認証データを作成することができる。なお、本システムで作成した本人認証データは、例えば文書改竄防止システムや認証文書確認システムの起動時の本人確認用のデータとすることができる。

【００４１】次に、請求項１０に対応する発明は、請求項９に記載された本人認証データ生成システムで生成した本人認証データ中のパスワードと、入力されたパスワードとを照合するパスワード照合手段と、指紋読取手段と、両パスワードが一致した場合には、指紋読取手段で指紋読み取りを行い、本人認証データ中の指紋データ

と、指紋読取手段にて読み取られた指紋データとを照合する指紋照合手段と、指紋照合が一致した場合には、本人認証データ中の指紋データから特徴抽出を行い指紋特徴データを生成する指紋特徴抽出手段と、指紋特徴抽出手段にて生成された指紋特徴データ及びパスワードから暗号鍵を生成する暗号鍵生成手段と、この生成された暗号鍵により本人認証データ内の暗号化された暗号鍵を復号して、生成された暗号鍵と復号した暗号鍵とを照合する暗号鍵照合手段と、暗号鍵照合が一致した場合には、この暗号鍵を用いて本人認証データ中の暗号化した秘密鍵を復号する秘密鍵復号手段とを備えた秘密鍵復号システムである。

【００４２】本発明はこのような手段を設けたので、例えば文書改竄防止システムや認証文書確認システムの起動時に本人を高い確実性をもって確認することができる。

【００４３】次に、請求項１１に対応する発明は、指紋読取手段と、指紋読取手段から読み取られる指紋データの境界を検出する境界検出手段と、境界検出手段により境界検出された指紋データをエンボス処理するエンボス手段と、エンボス手段によりエンボス処理された指紋データを輪郭トレースする輪郭トレース手段とを備えた指紋データ抽出装置である。

【００４４】本発明はこのような手段を設けたので、計算機で扱うことのできるデジタルデータとして指紋を抽出することができる。

【００４５】次に、請求項１２に対応する発明は、請求項１１に記載された指紋データ抽出装置から抽出された指紋データから複数の矩形領域を取り出す領域取出手段と、矩形領域のデータと予め登録した複数パターンとを比較し、何れかのパターンとマッチングするか否かを判定するパターンマッチング手段と、マッチングしたパターンに対応する数値を数列として並べ、当該数列を指紋特徴データとする手段とを備えた指紋特徴抽出装置である。

【００４６】本発明はこのような手段を設けたので、効果的に指紋データから指紋特徴データを抽出することができる。

【００４７】次に、請求項１３に対応する発明は、請求項１の発明を方法発明としたものであり、請求項１の発明と同様な効果を奏する。

【００４８】次に、請求項１４に対応する発明は、請求項２の発明を方法発明としたものであり、請求項２の発明と同様な効果を奏する。

【００４９】次に、請求項１５に対応する発明は、請求項３の発明を方法発明としたものであり、請求項３の発明と同様な効果を奏する。

【００５０】次に、請求項１６に対応する発明は、請求項１，２又は３記載の電子文書の改竄防止システムにて生成された認証データから第２の暗号化データを取出し、これを第２の秘密鍵に対応する第２の公開鍵で復号化する第２の復号化ステップと、第２の復号化ステップにより復号化されたデータから第１の暗号化データを取出し、これを第１の秘密鍵に対応する第１の公開鍵で復号化する第１の復号化ステップと、電子文書から特徴を抽出して照合用特徴データを生成する特徴抽出ステップと、第１の復号化ステップにより復号化されたデータから特徴データを取出し、これを照合用特徴データと照合する照合ステップと、照合ステップによる照合結果と、第２の復号化手段により復号化されたデータから取り出された外部認証データによって、外部認証者による認証の事実及び認証の日付を出力するステップとを有する認証文書確認方法である。

【００５１】本発明はこのような手段を設けたので、請求項５の発明と同様な効果を奏する。

【００５２】次に、請求項１７に対応する発明は、請求項１の発明を実現させるためのプログラムを格納した記録媒体についての発明であり、このプログラムを実行する計算機は、請求項１の発明における第２の暗号化手段を除いたものと同様な作用効果を奏する。

【００５３】次に、請求項１８に対応する発明は、請求項１，２又は３記載の電子文書の改竄防止システムにて生成された認証データから第２の暗号化データを取出し、これを第２の秘密鍵に対応する第２の公開鍵で復号化する第２の復号化手段と、第２の復号化手段により復号化されたデータから第１の暗号化データを取出し、これを第１の秘密鍵に対応する第１の公開鍵で復号化する第１の復号化手段と、電子文書から特徴を抽出して照合用特徴データを生成する特徴抽出手段と、第１の復号化手段により復号化されたデータから特徴データを取出し、これを照合用特徴データと照合する照合手段と、照合手段による照合結果と、第２の復号化手段により復号化されたデータから取り出された外部認証データによって、外部認証者による認証の事実及び認証の日付を出力する手段として、コンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【００５４】本発明はこのような手段を設けたので、このプログラムを実行する計算機は、請求項５の発明と同様な作用効果を奏する。

【００５５】次に、請求項１９に対応する発明は、請求項１の発明における処理が実行された結果として得られるデータ構造が記録された記録媒体についての発明である。

【００５６】次に、請求項２０に対応する発明は、請求項３の発明における処理が実行された結果として得られるデータ構造が記録された記録媒体についての発明である。

【００５７】次に、請求項２１に対応する発明は、認証付き電子文書から電子文書を取り出して、これに変更を

加えて、新たな電子文書を生成する文書変更手段と、認証付き電子文書から取り出された元の電子文書と新たな電子文書との変更点を抽出して変更箇所データを取得する差分抽出手段と、変更箇所データと新たな電子文書とをそれぞれ変更者認証する変更者認証手段と、変更者認証手段により認証された各データを外部の認証システムに送出するとともに、それぞれを外部認証された認証データを受け取って、受け取った各認証データ及び新たな電子文書に基づいて、認証付き変更箇所データと新たな認証付き電子文書を生成する認証手段とを備えた電子文書の改竄防止システムである。

【００５８】本発明はこのような手段を設けたので、変更された電子文書に新たな認証を付することができるとともに、変更部分のみのデータも認証することができ、変更電子文書の改竄を防止できる。また、外部認証を得ているので信頼性も高い。

【００５９】次に、請求項２２に対応する発明は、請求項２１に対応する発明において、変更者認証手段は、変更箇所データ及び又は新たな電子文書から特徴抽出して特徴データを出力する特徴抽出手段と、特徴データを、新たな電子文書を生成した変更者の暗号化鍵で暗号化して出力する暗号化手段とを備えた電子文書の改竄防止システムである。

【００６０】本発明はこのような手段を設けたので、変更箇所データ及び又は新たな電子文書そのものでなく、その特徴データを暗号化したものを認証データとするために認証元の特徴を残しつつ安全性を高めることができる。さらに認証データのデータ量を少なくできる。

【００６１】次に、請求項２３に対応する発明は、請求項２２に対応する発明において、変更者認証手段は、暗号化手段から出力されかつ新たな電子文書に対応する暗号化特徴データと、元の認証付き電子文書から取り出された以前の認証データとを結合して出力する結合手段を備えた電子文書の改竄防止システムである。

【００６２】本発明はこのような手段を設けたので、変更後の新たな電子文書に付する認証データに以前の認証データを含めることができ、変更毎の履歴とすることができる。また、各回の認証データを保持できる。

【００６３】次に、請求項２４に対応する発明は、請求項２２に対応する発明において、変更者認証手段は、特徴抽出手段により特徴抽出された特徴データと、元の認証付き電子文書から取り出された以前の認証データとを結合して出力する結合手段を備え、暗号化手段の暗号化対象として、結合手段からの出力データを特徴データに代えて入力する電子文書の改竄防止システムである。

【００６４】本発明はこのような手段を設けたので、請求項２３に対応する発明と同様な効果を他の手法で実現できる。

【００６５】次に、請求項２５に対応する発明は、請求項２１乃至２４のうち何れか１項に記載された認証手段により生成された認証付き変更箇所データと認証付き電子文書とを含む変更済電子文書から、認証付き変更箇所データ及び認証付き電子文書を取り出す分離手段と、請求項２１乃至２４のうち何れか１項に記載された文書変更手段、差分抽出手段、変更者認証手段及び認証手段と、認証手段により生成された新たな認証付き変更箇所データ及び新たな認証付き電子文書と、分離手段で分離された元の認証付き変更箇所データとに基づき、新たな変更済電子文書を生成する結合手段とを備えた電子文書の改竄防止システムである。

【００６６】本発明はこのような手段を設けたので、複数回の変更があっても変更後の電子文書を増やすことなく、かつ各変更毎の認証データを保持できる変更済電子文書を作成することができる。

【００６７】次に、請求項２６に対応する発明は、請求項２１乃至２４のうち何れか１項に記載された変更者認証手段により認証された各データを受け取る受入手段と、各データそれぞれに、少なくとも日付データ及び認証実行識別情報を結合する結合手段と、この結合手段により結合された各データを外部認証機関の暗号鍵によって暗号化して、外部認証された認証データを作成する暗号化手段とを備えた電子文書の外部認証システムである。

【００６８】本発明はこのような手段を設けたので、変更電子文書の確実かつ安全な認証を行うことができる。

【００６９】次に、請求項２７に対応する発明は、請求項２６に記載の外部認証システムにより外部認証された認証データを、外部認証機関の復号鍵で復号する復号化手段と、復号化手段により復号された認証データから、日付データ及び認証実行識別情報を取り出すデータ取出手段とを備えた認証文書確認システムである。

【００７０】本発明はこのような手段を設けたので、認証日付及び外部認証機関における認証情報（認証実行ＩＤ等）を取得することができる。

【００７１】次に、請求項２８に対応する発明は、請求項２７に対応する発明において、請求項２６に記載の外部認証システムにより外部認証された認証データが請求項２３に対応しかつ電子文書に対応するものである場合に、復号化手段により復号された認証データから、以前の認証データを取り出す認証データ取出手段を備えた認証文書確認システムである。

【００７２】本発明はこのような手段を設けたので、複数回の変更認証がなされている場合、各回の認証データひいては外部認証情報を取り出すことができる。

【００７３】次に、請求項２９に対応する発明は、請求項２８に対応する発明において、復号化手段により復号された認証データのうち、請求項２２の暗号化手段で暗号化された暗号データが入力されるとともに、当該暗号データを変更者の復号鍵で復号して特徴データを取り出す第２の復号化手段と、請求項２１の文書変更手段で得

られた新たな電子文書から特徴抽出して比較用特徴データを出力する特徴抽出手段と、第２の復号化手段で得られた特徴データと、特徴抽出手段で得られた比較用特徴データとを比較する照合手段とを備えた認証文書確認システムである。

【００７４】本発明はこのような手段を設けたので、電子文書が真正なものであるかを確認することができる。

【００７５】次に、請求項３０に対応する発明は、請求項２７に対応する発明において、請求項２６に記載の外部認証システムにより外部認証された認証データが請求項２４に対応しかつ電子文書に対応するものである場合に、復号化手段により復号された認証データを変更者の復号鍵で復号する第２の復号化手段と、第２の復号化手段で復号化された認証データから、以前の認証データを取り出す認証データ取出手段とを備えた認証文書確認システムである。

【００７６】本発明はこのような手段を設けたので、請求項２８に対応する発明と同様な効果を他の手法で得ることができる。

【００７７】次に、請求項３１に対応する発明は、請求項３０に対応する発明において、第２の復号化手段で復号化された認証データから、特徴データを取り出す分離手段と、請求項２１の文書変更手段で得られた新たな電子文書から特徴抽出して比較用特徴データを出力する特徴抽出手段と、分離手段で得られた特徴データと、特徴抽出手段で得られた比較用特徴データとを比較する照合手段とを備えた認証文書確認システムである。

【００７８】本発明はこのような手段を設けたので、請求項２９に対応する発明と同様な効果を他の手法で得ることができる。

【００７９】次に、請求項３２に対応する発明は、請求項２７に対応する発明において、請求項２６に記載の外部認証システムにより外部認証された認証データが請求項２２に対応しかつ変更箇所データに対応するものである場合に、復号化された認証データのうち、請求項２２の暗号化手段で暗号化された暗号データが入力されるとともに、当該暗号データを変更者の復号鍵で復号して特徴データを取り出す第２の復号化手段と、請求項２１の差分抽出手段で得られた変更箇所データから特徴抽出して比較用特徴データを出力する特徴抽出手段と、第２の復号化手段で得られた特徴データと、特徴抽出手段で得られた比較用特徴データとを比較する照合手段とを備えた認証文書確認システムである。

【００８０】本発明はこのような手段を設けたので、各回における変更箇所データの正当性が確認でき、ひいては電子文書が真正なものであるかを確認できる。

【００８１】次に、請求項３３に対応する発明は、請求項２５に記載された電子文書の改竄防止システムにより作成された変更済電子文書の変更部分についての認証確認を行うシステムであって、請求項２８又は３０の認証文書確認システムと、請求項３２の認証文書確認システムとを備えるとともに、複数回の変更を受けた最終的な変更済電子文書における認証付き電子文書から、最終変更回に関する認証データを取り出し、まずこれを請求項２６に記載の外部認証システムにより外部認証された認証データとして請求項２８又は３０の認証文書確認システムに入力し、最終変更回以外の各回については、請求項２８又は３０の認証文書確認システムから出力される以前の認証データを、請求項２６に記載の外部認証システムにより外部認証された認証データとして、順次、請求項２８又は３０の認証文書確認システムに入力し、また、複数回の変更を受けた最終的な変更済電子文書から、各回の認証付き変更箇所データを取り出し、この認証付き変更箇所データを変更箇所データ及び請求項２６に記載の外部認証システムにより外部認証された認証データに分離して、請求項３２の認証文書確認システムに入力し、請求項２８又は３０の認証文書確認システムから得られた日付データ及び認証実行識別情報と、請求項３２の認証文書確認システムから得られた日付データ及び認証実行識別情報とを各変更回毎に照合する変更済電子文書の認証確認システムである。

【００８２】本発明はこのような手段を設けたので、変更済電子文書の真実性を確認でき、証拠としての使用を可能とする。

【００８３】次に、請求項３４に対応する発明は、請求項３３に対応する発明において、請求項２９又は３１の認証文書確認システムを備えるとともに、最終的な変更済電子文書に包含される認証付き電子文書から取り出された認証データ及び新たな電子文書を、請求項２８又は３０の認証文書確認システムに代えて請求項２９又は３１の認証文書確認システムに入力する変更済電子文書の認証確認システムである。

【００８４】本発明はこのような手段を設けたので、より一層電子文書の証拠能力を高めることができる。

【００８５】次に、請求項３５に対応する発明は、請求項２１に対応する発明をコンピュータに実現させるプログラムを記録した記録媒体である。

【００８６】この記録媒体から読み出されたプログラムにより制御されるコンピュータは、請求項２１の電子文書の改竄防止システムとして機能する。

【００８７】次に、請求項３６に対応する発明は、請求項２２に対応する発明をコンピュータに実現させるプログラムを記録した記録媒体である。

【００８８】この記録媒体から読み出されたプログラムにより制御されるコンピュータは、請求項２２の電子文書の改竄防止システムとして機能する。

【００８９】次に、請求項３７に対応する発明は、請求項２７に対応する発明をコンピュータに実現させるプログラムを記録した記録媒体である。

【００９０】この記録媒体から読み出されたプログラム

により制御されるコンピュータは、請求項２７の認証文書確認システム電子文書の改竄防止システムとして機能する。

【００９１】

【発明の実施の形態】次に、本発明の実施の形態について説明する。

【００９２】［第１～第１３の実施形態についての説明］図１は本発明の各実施形態における電子文書の改竄防止システム及び方法の全体的な構成を示す図である。

【００９３】公衆回線や専用回線を用いたネットワーク１００が構成され、当該ネットワークに文書認証システム１０１や外部認証機関９９の外部認証システム１０２、認証文書確認システム１０３が接続されている。

【００９４】文書認証システム１０１は、認証対象となる電子文書に関する当該システム使用者作成の所定情報（使用者の鍵で暗号化したことによる一種の使用者認証を含む）をネットワーク１００を介して外部認証システム１０２に送付し、この所定情報を元に外部認証システム１０２で作成された認証のための情報の返信を受け認証電子文書を作成する。また、後の実施形態でも説明するが、複数の文書認証システム１０１でそれぞれ異なるシステム使用者に加工（暗号化や認証情報付加等であり、各使用者による実質的な認証になっている）された所定情報が外部認証システム１０２に送付される場合もある。

【００９５】一方、認証文書確認システム１０３は、上記認証電子文書の正当性を確認するためのシステムであり、ネットワーク１００を介し文書認証システム１０１等から確認対象の認証電子文書を受信する。

【００９６】文書認証システム１０１、外部認証システム１０２及び認証文書確認システム１０３は、ワークステーションやパーソナルコンピュータ等の計算機に表示装置、入力装置、あるいは例えば指紋読取り機等を付加したものであり、基本的にはその動作プログラムが相違することで異なる各機能を実現する。したがって、図１に示すように、例えば文書認証システム１０１と認証文書確認システム１０３とが同一の計算機上に構成される場合もある。

【００９７】さらに、文書認証システム１０１と外部認証システム１０２とを同一計算機、あるいはＬＡＮ等で接続される計算機上に構成させ、外部認証機関において認証作業のすべてを行うようにすることも可能である。

【００９８】本発明にかかわる電子文書の改竄防止システム及び方法は、これらの文書認証システム１０１、外部認証システム１０２及び認証文書確認システム１０３を適宜組み合わせ、あるいはその一部機能を適宜組み合わせてなるものである。

【００９９】また、上記場合は、ネットワークを介した情報の瞬時転送を前提とした場合を説明しているが、図１に示すように、フロッピーディスク等の記録媒体９７，９８を介して文書認証システム１０１～外部認証システム１０２間、あるいは文書認証システム１０１～認証文書確認システム１０３間で必要情報（所定情報や電子文書）の交換を行うことも可能である。

【０１００】全体的には以上のシステム構成を有する電子文書の改竄防止システム及び方法について、その各実施形態を以下に説明する。

【０１０１】（第１の実施の形態）本実施形態は改竄を防止できる電子文書の作成システム及び方法に関するものである。

【０１０２】図２は本発明の第１の実施の形態に係る電子文書の改竄防止システムに適用される文書認証システムのハードウエア構成例を示すブロック図である。

【０１０３】文書認証システムは、計算機１１０に、表示装置１１１、入力装置１１２、印刷装置１１３、外部記憶装置１１４、指紋読取り機６４、スキャナ１１５が接続されてなっている。

【０１０４】計算機１１０においては、ＣＰＵバス１１６にＣＰＵ１１７、ＲＯＭ１１８、ＲＡＭ１１９が接続され、さらに、ＣＰＵバス１１６に接続される各インターフェース手段１２０，１２１，１２２，１２３，１２４，１２５，１２６，１２７を介してそれぞれハードディスク装置１２８、通信装置１２１、表示装置１１１、入力装置１１２、印刷装置１１３、外部記憶装置１１４、指紋読取り機６４、スキャナ１１５が接続されている。

【０１０５】ＲＯＭ１１８は、コンピュータ１１０を起動しオペレーティングシステム（ＯＳ）等を立ち上げるのに用いられるブート処理プログラム等が格納されている。

【０１０６】また、ハードディスク装置１２８には、プログラム格納部１３０及びデータ格納部１３１が設けられている。プログラム格納部１３０は、ＯＳや、文書認証システム１０１を実現するプログラム等を格納し、データ格納部１３１は、電子文書、認証付き電子文書、その他各種情報を格納する。

【０１０７】ＲＡＭ１１９は、いわゆる主記憶に使用される。すなわち、ＣＰＵ１１７による各種処理のための作業領域１３２を備え、またＣＰＵ１１７を制御する文書認証プログラム１３３を格納している。

【０１０８】この文書認証プログラム１３３は、ハードディスク装置１２８のプログラム格納部１３０から呼び出され、ＲＡＭ１１９内に格納されるものである。

【０１０９】ＣＰＵ１１７は、ＲＡＭ１１９内の文書認証プログラム１３３に従って各部を制御し、文書認証システム１０１を実現する。つまり、ＲＡＭ１１９（特に文書認証プログラム１３３）やハードディスク装置１２８等のソフトウエア資源とＣＰＵ１１７等の図２のハードウエア資源とが結合して文書認証システム１０１の各機能実現手段が構成される。本実施形態及び以下の各実

施形態における処理説明図や流れ図等に表現される各手段（各処理）あるいは図示しない各手段（各処理）は、このような機能実現手段であり、主として文書認証プログラム１３３に従うＣＰＵ１１７の動作によるものである。

【０１１０】通信装置１２９は、外部認証システム１０２と間あるいは認証文書確認システム１０３と間の通信を行うものである。電子文書や各種情報の授受が行われる。

【０１１１】外部記憶装置１１４は、電子文書、認証付き電子文書、その他各種情報を可搬な記録媒体に格納し、特に認証付き電子文書の保存、送付等を便利かつ容易にするものである。外部記憶装置１１４としては、例えばフロッピーディスク装置、光磁気ディスク装置（ＭＯ）、ＣＤ－Ｒ、ＣＤ－Ｒ／ＷあるいはＤＶＤ等が用いられる。

【０１１２】指紋読取り機６４は、人間の指紋情報を読み取る装置である。システム使用者の認証や暗号情報作成等のために用いられる。

【０１１３】スキャナ１１５は、印鑑等の図形をイメージ情報として読み取る装置である。

【０１１４】次に外部認証システムのハードウエア構成について説明する。

【０１１５】図３は本実施形態の電子文書の改竄防止システムに適用される外部認証システムのハードウエア構成例を示すブロック図であり、図２と同一部分には同一符号を付してその説明を省略する。

【０１１６】外部認証システム１０２は、文書認証システム１０１と同様な計算機システムから構成される。文書認証システム１０１との相違点は、ハードディスク装置１２８のプログラム格納部１３０に格納される動作プログラムである。この動作プログラムが呼び出され、ＲＡＭ１１９内に外部認証プログラム１３４として格納される。ＣＰＵ１１７は、この外部認証プログラム１３４に従って各部を制御し、外部認証システム１０２が実現される。また、ソフトウエア資源（特に外部認証プログラム１３４）とハードウエア資源とが結合して機能実現手段が構成される点も文書認証システム１０１の場合と同様である。

【０１１７】次に、図４を用いて電子文書の改竄防止システムの各機能について説明する。図４は本実施形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図である。

【０１１８】この電子文書の改竄防止システムは、文書認証システム１０１と外部認証システム１０２とから構成されている。

【０１１９】文書認証システム１０１は、認証すべき電子文書１から特徴データ３Ｄを抽出し暗号化するとともに、この暗号化データ６について認証を与える外部認証機関の外部認証システム１０２から合成データ１０を受け取り、これを上記電子文書１に付与して認証付き電子文書１２を作成する。

【０１２０】このために文書認証システム１０１は、見出し３Ｈの取出編集手段（図示せず）と、電子文書１から特徴抽出を行って特徴データ３Ｄを生成する特徴抽出手段２と、特徴データ３Ｄを第１の秘密鍵４（＃１）（以下、複数存在し得る同種類の構成やデータには、場合により＃１，＃２，．．あるいは第１の、第２の、．．と記して区別する）にて暗号化し暗号化データ６Ｄ（＃１）を生成する暗号化手段６と、見出し３Ｈと暗号化データ６Ｄとを結合する手段（図示せず）と、結合された見出し付き暗号化データ６を外部認証システム１０２に送信する通信手段（図示せず）と、外部認証システム１０２から受け取った合成データ１１を電子文書１に付与して認証付き電子文書１２を作成し電子媒体に保存する手段（図示せず）を備えている。

【０１２１】一方、外部認証システム１０２は、文書認証システム１０１から受け取った見出し付き暗号データ６を分離手段（図示せず）で分離し、このうちの暗号データ７Ｄに外部認証データ７Ａ（＃１）を付与しこれを暗号化手段９を用いて第２の秘密鍵８（＃２）にて暗号化した後、この暗号データ１０Ｄと見出し１０Ｈからなる合成データ１０を結合手段（図示せず）で結合して通信手段（図示せず）により文書認証システム１０１に送信する。

【０１２２】なお、本実施形態では、各データの暗号化方式として秘密鍵と公開鍵を使用したＲＳＡ方式が用いられるが、他の暗号化方式（ＤＥＳ方式等）を用いてもよい。

【０１２３】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図４及び図５を用いて説明する。

【０１２４】図５は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【０１２５】まず、文書認証システム１０１において電子文書１のデータが読み込まれ（Ｓ１）、その文書データから文書タイトルや日付等の見出し３Ｈのデータに使用できる部分が取り出され、更に補足説明を追加する為に編集が行される。こうして見出し３が作成される（Ｓ２）。なお、見出し３には例えば第７実施形態で説明する文書作成者の電子印鑑や電子署名等も含まれる。

【０１２６】次に、特徴抽出手段２により電子文書１から特徴が抽出され特徴データ３Ｄが作成される（Ｓ３）。ここで、特徴データ３Ｄは、例えば電子文書の１ビットが変化しても異なった値となるような電子文書自体の特徴を示すデータである。一方、見出し３Ｈは特徴データ３Ｄがどの電子文書のものであるかを分かるようにする為に追加されるデータである。見出し３Ｈと特徴データ３Ｄは合成データ（見出し付き特徴データ３）として対応が取られるようにする。

【０１２７】次に、暗号化手段５により秘密鍵４（＃１）が用いられ、特徴データ３Ｄが暗号化され第１の暗号データ６Ｄが生成される（Ｓ４）。なお、第１の秘密鍵４は電子文書１の作成者が保有する秘密鍵であり、他人には知らせないようにしたものである。

【０１２８】次に、見出し６Ｈと暗号データ６Ｄを結合し見出し付き暗号データ６として対応が取られる（Ｓ５）。なお、見出し６Ｈは見出し３Ｈと同じものである。このようにしてできた見出し付き暗号データ６は外部認証機関の外部認証システム１０２に送信される（Ｓ６）。なお、この送信は、本実施形態では公衆回線や専用回線を介し、ネットワーク１００に伝送されるが、例えばフロッピーディスク等の電子媒体に記録して郵送等してもよい。

【０１２９】一方、外部認証機関では、文書認証システム１０１からの見出し付き暗号データ６が受信される（Ｓ７）。

【０１３０】外部認証システム１０２では見出し付き暗号データ６が見出し７Ｈと暗号データ７Ｄに分解される（Ｓ８）。このうちの暗号データ７Ｄに外部認証データ７Ａが結合される（Ｓ９）。この外部認証データ７Ａは、文書認証システム１０１が認証を要求してきたデータについて第三者である外部認証機関が認証したことを示す情報であり、認証した日付データが含まれる。

【０１３１】次に、暗号化手段９により第１の暗号データ７Ｄ（＃１）と外部認証データ７Ａ（＃１）が纏められ、秘密鍵８で暗号化される（Ｓ１０）。こうして第２の暗号データ１０Ｄ＃２が生成される。これにより第２の暗号データ１０Ｄ（＃２）は作成者の秘密鍵４と外部認証機関の秘密鍵８で二重に鍵が掛けられたデータとなり、かつそれぞれ独自のデータが含まれる。

【０１３２】さらに、第２の暗号データ１０Ｄは見出し１０Ｈと合成されて合成データ１０となり、その取り扱いが容易に形になる（Ｓ１１）。なお、見出し１０Ｈは見出し３Ｈと同じ内容である。そして、合成データ１０は外部認証システム１０２から第三者認証を要求する作成者の文書認証システム１０１にネットワーク１００を介して返信される（Ｓ１２）。

【０１３３】文書認証システム１０１では、合成データ１０が合成データ１１として受け取られる（Ｓ１３）。そして、この合成データ１１は電子文書１と合成されて認証付き電子文書１２が生成される。このような結合をすればデータ取り扱いが容易になる。生成された認証付き電子文書１２は任意の場所の電子媒体に保管することができ、何れの場所に保管されても認証機能を発揮することになる。なお、ここでいう結合というのは、単に同一の記録媒体に合成データ１１と電子文書１とを記録する場合や、両者の関連付けを示す他のデータを作成する場合等、様々な場合を含むものである。この結合する手段は、請求項における電子文書の認証データとする手段の一例でもある。

【０１３４】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、本人により電子署名された文書を外部認証機関が認証する手順を踏むことにより、外部認証機関の認証日付にはまさしく本人が文書を作成していたことが証明される。また、たとえ電子署名がない場合であっても、文書作成者本人の秘密鍵４で特徴データの暗号化がなされ、これに対応する公開鍵で復号化されることになるので、何れにしても文書作成者の作成になる文書であることが認証される。

【０１３５】また、文書本体の改竄を行うと改竄後の文書から抽出されるべき特徴データが変化し、先に認証用に抽出された特徴データ３Ｄと異なるものになることによって元文書の改竄の事実が検出できる。一方、先に認証用に抽出された特徴データ３Ｄは、外部認証機関の認証データ７Ａと共に認証機関の秘密鍵８で暗号化されているので、認証付き電子文書１２に付されている暗号データ１１Ｄの改竄は不可能である。したがって、たとえ本人であっても外部認証後には文書改竄が不可能になる。

【０１３６】これにより裁判の場で文書の正当性が証明できる，証拠能力のある電子文書が生成でき、従来紙で保存していた重要文書や、証拠書類を電子化する事が可能となる。また、従来の紙の文書でも改竄の有無を判定するには高度な技術が必要とされたが、本発明になる電子文書の改竄防止システムでは電子的な手順を踏むだけで改竄の有無を確認できるので、改竄の有無を容易に証明できる。さらに電子化により保管場所が削減されると共に、遠隔地への文書電送が瞬時に行えるようになり、コンピュータによる検索が行えるようになる。こうして、商取引の信用向上、取引の迅速化を図ることができる。

【０１３７】また、本実施形態の文書改竄防止システムでは、文書認証システム１０１や外部認証システム１０２においてそれぞれ電送データの暗号化が行われるので、ネットワーク１００として公衆回線を用いても安全である。

【０１３８】さらに、外部認証機関が認証した外部認証データを元の電子文書に結合して認証付き電子文書１２の形で管理するようにしたので、電子文書を保存する時の扱いが楽になる。

【０１３９】（第２の実施の形態）本実施形態では第１の実施形態で認証した認証付き電子文書１２が真正なものであることを確認し、また外部認証機関の付した認証日付等の認証情報を取り出すシステムについて説明する。

【０１４０】この電子文書の改竄防止システムは、図１に示した認証文書確認システム１０３として構成されるものである。

【０１４１】図６は本発明の第２の実施の形態に係る電

子文書の改竄防止システムに適用される認証文書確認システムのハードウエア構成例を示すブロック図であり、図２と同一部分には同一符号を付してその説明を省略する。

【０１４２】認証文書確認システム１０３は、文書認証システム１０１と同様な計算機システムから構成される。文書認証システム１０１との相違点は、ハードディスク装置１２８のプログラム格納部１３０に格納される動作プログラムである。この動作プログラムが呼び出され、ＲＡＭ１１９内に認証文書確認プログラム１３５として格納される。ＣＰＵ１１７は、この認証文書確認プログラム１３５に従って各部を制御し、認証文書確認システム１０３が実現される。また、ソフトウエア資源（特に認証文書確認プログラム１３５）とハードウエア資源とが結合して機能実現手段が構成される点も文書認証システム１０１の場合と同様である。

【０１４３】次に、図７を用いて電子文書の改竄防止システムの各機能について説明する。図７は本実施形態の電子文書の改竄防止システムに適用される認証文書確認システム１０３の機能構成及び処理流れの一例を示す図であり、図４と同一部分には同一符号を付して説明を省略する。

【０１４４】この認証文書確認システム１０３は、認証付き電子文書１２から取り出した特徴データ１８Ｄと認証付き電子文書１２から合成データ１１を取り除いた電子文書１９から抽出される特徴データ２１とを照合し、電子文書の同一性を行うとともに、認証データ（暗号データ１１Ｄ）より取り出された外部認証データ１５Ａから外部認証機関９９による認証の事実及びその認証日付を確認する。

【０１４５】このために認証文書確認システム１０３には、外部記憶装置１１４やハードディスク装置１２８に格納された認証付き電子文書１２から見出し１１Ｈ及び暗号データ１１Ｄを取り出す手段（図示せず）と、暗号データ１１Ｄを外部認証システム１０２の第２の公開鍵１３（＃２）により復号化する復号化手段１４と、この復号化により得られたデータのうちの外部認証データ１５Ａ（＃１）により日付認証１５Ａ－Ｄ及び外部認証機関９９の認証確認を行う手段（図示せず）と、復号化手段１４で復号化されたデータのうちの暗号データ１５Ｄを文書認証システム１０１の第１の公開鍵１６（＃１）で復号化する復号化手段１７とが設けられている。さらに、認証データを取り除いた電子文書１９から特徴データ２１を取り出す特徴抽出手段２０と、この特徴データ２１と，復号化手段１７で復号化された見出し付き特徴データ１８から取り出した特徴データ１８Ｄとを照合し、電子文書１９が電子文書１と同一であるか否かの同一性判定２２－Ｊを行う照合手段とが設けられている。

【０１４６】本実施形態では、秘密鍵と公開鍵を使用した暗号としてはＲＳＡ方法が用いられるが、他の暗号化方式（ＤＥＳ方式等）を用いてもよい。なお、図７に示す認証文書確認システム１０３は電子文書１の作成者のシステムでも第三者のシステムでもかまわない。

【０１４７】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図７及び図８を用いて説明する。

【０１４８】図８は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【０１４９】まず、外部記憶装置１１４、ハードディスク装置１２８から、あるいはネットワーク１００を介して電子文書１２が読み込まれ（Ｔ１）、合成データ１１が取り出される（Ｔ２）。

【０１５０】合成データ１１の中から更に認証データとして機能する第２の暗号データ１１Ｄ（＃２）が取り出される（Ｔ３）。第２の公開鍵１３（＃２）を使用して復号化手段１４で復号が行われる（Ｔ４）。なお、第２の公開鍵１３（＃２）は外部認証機関９９の公開鍵であり、第２の秘密鍵８（＃２）に対応するものである。これによって第１の暗号データ１５Ｄ（＃１）と外部認証データ１５Ａ（＃１）とが取り出される。

【０１５１】次に、見出し付き認証データ１５から暗号データ１５Ｄと外部認証データ１５Ａとが分離される（Ｔ５）。なお、暗号データ１５Ｄは図４の暗号データ６Ｄと内容が同一のものである。また、外部認証データ１５Ａは図４の外部認証データ７Ａと内容が同一のものである。さらに、見出しデータ１５Ｈは図４の見出しデータ３Ｈと内容が同一のものである。

【０１５２】次に、復号された外部認証データ１５Ａから日付認証データ１５Ａ－Ｄが取り出され、外部認証機関が合成データ６の認証を行った日付が確認される（Ｔ６）。

【０１５３】一方、第１の暗号データ１５Ｄ（＃１）は第１の公開鍵１６（＃１）で復号化手段１７によって復号され（Ｔ６）、第１の特徴データ１８Ｄが生成される。第１の公開鍵１６（＃１）は電子文書の作成者の公開鍵であり、第１の秘密鍵４（＃１）に対応するものである。なお、特徴データ１８Ｄは第１の特徴データ３Ｄ（＃１）と内容が同一のものである。

【０１５４】次に、電子文書１２から合成データ１１を除いた電子文書１９が取り出される（Ｔ８）。この電子文書１９は元の電子文書１に対応するものである。さらに、電子文書１９から特徴抽出手段２０により特徴データ２１が取り出される（Ｔ９）。特徴抽出手段２０は特徴抽出手段２と同一の手段であり、電子文書１９の内容が電子文書１と同一であれば同一の特徴データが生成される。

【０１５５】次に、特徴データ１８Ｄと特徴データ２１とが照合手段２２により照合され（Ｔ１０）、照合結果が同一かどうかを示す同一性判定結果２２－Ｊが出力される。同一性判定結果２２－Ｊが判定良（一致）であれ

ば（Ｔ１１）、日付認証データ１５Ａ－Ｄの日付で認証された本人作成の文書である事が証明される。そこで、ステップＴ６で取り出した日付認証と共に文書同一である旨が表示装置１１１に表示される（Ｔ１３）。

【０１５６】一方、同一性判定結果２２－Ｊが判定不良（不一致）であれば（Ｔ１１）、不一致が表示される。

【０１５７】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、暗号化特徴データの付加、本人電子署名及び外部認証機関の認証がなされた電子文書から外部認証機関の外部認証データを取出し、また付加されている特徴データと電子文書本体からの特徴データとを文書作成者の公開鍵１６を用いて照合することで、外部認証機関の認証日付にはまさしく本人が文書を作成していたことが証明される。

【０１５８】電子文書本体の改竄を行うと、電子文書１９から抽出される特徴データ２１が変化することにより、一方、第１の特徴データ３Ｄ，１８Ｄは外部認証機関９９によって改竄を防止される事によって、本人であっても外部認証後には文書改竄が不可能になる。これにより裁判の場で文書の正当性が証明でき、従来紙で保存していた重要文書や、証拠書類を電子化する事が可能となる。

【０１５９】また、従来の紙の文書でも改竄の有無を判定するには高度な技術が必要とされたが、上記照合処理により電子文書の改竄防止システムでは容易に改竄の有無を証明できる。さらに、電子化により保管場所が削減されると共にネットワークを介して遠隔地への電送が瞬時に行い得る。したがって、さらに、コンピュータによる検索も可能である。

【０１６０】また、本実施形態の文書改竄防止システムでは、文書認証システム１０１や外部認証システム１０２においてそれぞれ電送データの暗号化が行われるので、ネットワーク１００として公衆回線を用いても安全である。

【０１６１】さらに、外部認証機関が認証した認証データを元の電子文書に結合する事により、文書を保存する時の扱いが楽になる。

【０１６２】（第３の実施の形態）本実施形態の電子文書の改竄防止システム及び方法では、一旦作成された認証付き電子文書１２に付された合成データ１１にさらに外部認証データを付し、暗号化をかけ直す。これにより改竄防止を強化した電子文書を生成し、認証付き電子文書１２の作成から長期間を経た認証データの秘匿性を維持するものである。

【０１６３】図９は本発明の第３の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図４及び図７と同一部分には同一符号を付し、その説明を省略する。また、本実施形態のシステムには、図２及び図３に示す文書認証システム１０１及び外部認証システム１０２が用いられており、本実施形態の独自な機能部分は、文書認証プログラム１３３あるいは外部認証プログラム１３４に修正が加えられたことによるものである。

【０１６４】この電子文書の改竄防止システムは、図１に示す文書認証システム１０１と外部認証システム１０２とから構成されている。

【０１６５】文書認証システム１０１は、電子文書１２から合成データ１１を取出し、外部認証システム１０２に送付する手段（図示せず）と、電子文書１２から認証データ１１を取り除いて元の電子文書としたものに外部認証システム１０２から受け取った見出し付き暗号データ２７を認証データとして付加して認証付き電子文書２８とする手段（図示せず）とが加えられる他、第１の実施形態と同様に構成されている。

【０１６６】一方、外部認証システム１０２は、文書認証システム１０１からの合成データ１１に外部認証データ２３Ａを付加するとともに、暗号データ２３Ｄ（暗号データ１１Ｄと同一）と外部認証データ２３Ａとを第３の秘密鍵２４（＃３）で暗号化する暗号化手段２５と、この暗号化された暗号データ２６Ｄと見出し２６Ｈからなる見出し付き暗号データ２６を文書認証システム１０１に送信する手段（図示せず）とが加えられる他、第１の実施形態と同様に構成されている。なお、第３の秘密鍵２４（＃３）は、外部認証機関９９のもう一つの秘密鍵である。

【０１６７】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図９及び図１０を用いて説明する。

【０１６８】図１０は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【０１６９】まず、文書認証システム１０１において、外部記憶装置１１４、ハードディスク装置１２８から、あるいはネットワーク１００を介して電子文書１２が読み込まれ（Ｕ１）、認証データである合成データ１１が取り出される（Ｕ２）。この合成データ１１が外部認証機関９９の外部認証システム１０２にネットワーク１００を介して送信される（Ｕ３）。

【０１７０】）。

【０１７１】次に、外部認証システム１０２において、ステップＵ３で送信された合成データ１１（認証データ）が受信される。次に受け取った合成データ１１が見出し２３Ｄと暗号データ２３Ｄに分離される（Ｕ５）。ここで見出し付き認証データ２３に外部認証データ２３Ａが追加される。なお、外部認証データ２３Ａは、第１の実施形態の外部認証データ７Ａと同様なものであり、認証日等の情報が含まれる。

【０１７２】次に、暗合データ２３Ｄと外部認証データ２３Ａが結合され（Ｕ６）、この結合データが秘密鍵２４（＃３）にて暗号化され暗号データ２６Ｄが生成される（Ｕ７）。なお、この秘密鍵２４は、外部認証機関９

９の秘密鍵であり、例えばＲＳＡ方式に対応するものである。

【０１７３】次に、見出し２６Ｈと暗合データ２６Ｄとが結合されてなる認証データである暗号データ２６が生成され（Ｕ８）、当該データ２６が文書認証システム１０１にネットワーク１００を介して送信される（Ｕ９）。

【０１７４】外部認証機関９９から送信された暗号データ２６が文書認証システム１０１により受信される（Ｕ１０）。これが見出し付き暗号データ２７とされ、電子文書１２から暗号データ１１を取り除いた元の電子文書に合成されて認証付き電子文書２８が生成される（Ｕ１１）。こうして改竄防止が強化された電子文書が生成されることになる。なお、電子文書２８は外部記憶装置１１４やハードディスク装置１２８、その他の任意の場所の電子媒体に保管することができる。

【０１７５】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、電子文書１２から取り出した合成データ１１に再度外部認証機関９９の認証を与え、暗号をかけ直して認証付き電子文書２８を生成するようにしたので、改竄防止を強化した文書２８を作成することができる。

【０１７６】したがって、暗号技術の進歩により、最初の暗号が解読される恐れがある年数を経過する前に、更に新しい暗号により文書１の改竄防止を強化することでき、たとえ長期間の電子文書保管を行っても、裁判の場で文書の正当性が証明できるようになる。

【０１７７】なお、本実施形態では、電子文書１２の如く１度の認証の電子文書を再認証する場合を説明したが、本実施形態の手法を用いて電子文書２８をさらに再認証するようにしてもよい。このように再認証を繰り返し認証の回数を重ねる事によって、電子文書１の保管年限が延長でき、事実上無限長とすることができる。したがって、本実施形態では、公開鍵方式（ＲＳＡ）の暗号方式で際認証する場合を説明したが、その時々に開発された最も解読困難な暗号方式で適宜再認証（再暗号化）することが適当である。

【０１７８】（第４の実施の形態）本実施形態では第３の実施形態で再認証し改竄防止を強化した認証付き電子文書２８が真正なものであることを確認し、また外部認証機関の付した各認証日付等の認証情報を取り出すシステムについて説明する。

【０１７９】図１１は本発明の第４の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図４、図７及び図９と同一部分には同一符号を付し、その説明を省略する。また、本実施形態のシステムには、図６に示す認証文書認証システム１０３が用いられており、本実施形態の独自な機能部分は、認証文書確認プログラム１３５に修正が加えられたことによるものである。

【０１８０】この電子文書の改竄防止システムは、図１に示した認証文書確認システム１０３として構成されるものである。

【０１８１】認証文書確認システム１０３は、認証付き電子文書２８から取り出した認証データについて３回の復号処理を施して特徴データ１８Ｄを取出し、電子文書１９から取り出した特徴データ２１との照合を行うとともに、その過程で、外部認証機関９９による２回の認証についてそれぞれの認証日付及び外部認証の旨の確認を行うようになっている。

【０１８２】このために、認証文書確認システム１０３には、認証付き電子文書２８から見出し付き暗号データ２７を取り出す手段（図示せず）と、外部認証機関９９の公開鍵２９（＃３）により暗号データ２７Ｄを復号化する復号化手段３０と、復号化された外部認証データ３１Ａから外部認証機関９９の認証確認を行い日付認証３１Ａ－Ｄを取り出す手段（図示せず）とが設けられる他、図７に示す第２の実施形態と同様に構成されている。なお、復号化手段１４が復号するデータは、暗号データ３１Ｄである。

【０１８３】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図１１及び図１２を用いて説明する。

【０１８４】図１２は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【０１８５】まず、認証文書確認システム１０３において、外部記憶装置１１４、ハードディスク装置１２８から、あるいはネットワーク１００を介して認証付きの電子文書２８が読み込まれる（Ｖ１）。次に、電子文書２８から認証データである見出し付き暗号データ２７が取出される（Ｖ２）。さらに見出し付き暗号データ２７から暗号データ２７Ｄが分離される（Ｖ３）。復号化手段３０により、この分離された暗号データ２７Ｄが外部認証機関の公開鍵２９（＃３）で復号化される（Ｖ４）。これによって、暗号データ３１Ｄと第２の外部認証データ３１Ａの合成データが生成される。ここで認証データに改竄がなければ、暗号データ３１Ｄは、暗号データ１１Ｄ又は１０Ｄと同じものであり、第２の外部認証データ３１Ａは、外部認証データ２３Ａと同じものである。

【０１８６】次に、暗号データ３１Ｄと第２の外部認証データ３１Ａとが分離される（Ｖ５）。さらに、外部認証データ３１Ａから日付認証３１Ａ－Ｄが取出され、この２回目の外部認証機関９９の認証が確認される（Ｖ６）。一方、暗号データ３１Ｄは外部認証機関９９の公開鍵１３（＃２）を使用して復号化手段１４により復号され、暗号データ１５Ｄと外部認証データ１５Ａの合成データが生成される（Ｖ７）。ここで認証データに改竄がなければ、暗号データ１５Ｄは、暗号データ６Ｄ又は７Ｄと同じものであり、外部認証データ１５Ａは、１回目の外部認証データ７Ａと同じものである。

【０１８７】次に、上記合成データが外部認証データ１５Ａと暗号データ１５Ｄとに分離され（Ｖ８）、外部認証データ１５Ａからは日付認証データ１５Ａ－Ｄが取出される（Ｖ９）。これにより１回目の外部認証機関９９による認証が確認される。

【０１８８】次に、暗号データ１５Ｄが作成者の公開鍵１６（＃１）を使用して復号化手段１７により復号化され、見出し付き特徴データ１８が生成される（Ｖ１０）。さらに、見出し１８Ｈと特徴データ１８Ｄとに分離される（Ｖ１１）。

【０１８９】一方、認証付き電子文書２８から、見出し付き暗号データ２７が取り除され、この元の電子文書１９から特徴抽出手段２０により特徴データ２１が抽出される（Ｖ１２）。そして、ステップＶ１１で分離された特徴データ１８Ｄと、特徴データ２１とが照合手段２２により照合され、同一性判定データ２２－Ｊが生成される（Ｖ１３）。

【０１９０】照合結果である同一性判定データ２２－Ｊにより、電子文書１９と電子文書１とが同一かどうかが判定され（Ｖ１４）、不一致と判断された場合には表示装置１１１から不一致が表示される（Ｖ１５）。一方、同一と判断された場合には、認証日付３１Ａ－Ｄ及び１５Ａ－Ｄとが表示され、さらに同一である旨の表示が行われる（Ｖ１６）。こうして、改竄防止を強化した電子文書の同一性判定が終了する。

【０１９１】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、外部認証機関９９において期間をおいて２度に渡って認証され暗号化された認証付き電子文書２８について、同一性を照合し外部認証を確認するようにしたので、改竄防止を強化した電子文書２８の同一性の判定を容易に行う事ができる。また、暗号解読の恐れが有る年数を経過する前に更に新しい暗号による文書の改竄防止ができるので、長期間の電子文書保管を行っても、裁判の場で文書の正当性が証明できるようになる。

【０１９２】本実施形態では、電子文書２８の如く１度の再認証（合計２回の外部認証）の電子文書２８の同一性判定を行う実施例を説明したが、電子文書２８を更に再認証した文書の同一性判定をしてもよい。認証の回数を重ねた場合は、復号の回数を重ねる事で電子文書の同一性判定が行える。

【０１９３】（第５の実施の形態）本実施形態では、第１又は第３の実施形態で説明した電子文書の改竄防止システムを利用した電子契約書作成システムについて説明する。

【０１９４】図１３は本発明の第５の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図４、図７、図９及び図１１と同一部分には同一符号を付し、その説明を省略する。また、本実施形態のシステムには、図２及び図３に示す文書認証システム１０１及び外部認証システム１０２が用いられており、本実施形態の独自な機能部分は、文書認証プログラム１３３あるいは外部認証プログラム１３４に修正が加えられたことによるものである。

【０１９５】この電子文書の改竄防止システムは、契約者の一方である甲が使用する文書認証システム１０１（以下、甲システム１０１ａともいう）と、契約者の他方である乙が使用する文書認証システム１０１（以下、乙システム１０１ｂともいう）と、外部認証システム１０２とから構成されている。また、この電子文書の改竄防止システムは、甲乙間での契約を行うための電子契約書作成システムともなっている。なお、甲システム１０１ａと、乙システム１０１ｂと、外部認証システム１０２とは図１に示すようにネットワークで接続されている。

【０１９６】甲システム１０１ａは、秘密鍵４（＃１）として甲の秘密鍵４（甲）を用い、また見出し付き暗号データ６を外部認証システム１０２に代えて乙システム１０１ｂに送信する。さらに、甲システム１０１ａは、外部認証システム１０２から受け取る合成データ１１として見出し付き暗号データ４０を受け取り、電子文書１に付して電子契約書である認証付き電子文書４１を作成する他、第１又は第３の実施形態の文書認証システム１０１と同様に構成されている。

【０１９７】一方、乙システム１０１ｂは、甲システム１０１ａから受け取った見出し付き暗号データ６の中の暗号データ３２Ｄに乙の認証データ３２Ａを付加した結合データを生成し、見出し付き認証データ３２を作成する手段（図示せず）と、この結合データを乙の秘密鍵３３（乙）で暗号化する暗号化手段３４と、見出し付き認証データ３２の見出し３２Ｈ（３５Ｈ）と暗号化手段３４で暗号化された暗号データ３５Ｄとを結合して電子署名３５を作成する手段（図示せず）と、この電子署名３５を外部認証システムにネットワークを介して送信する手段（図示せず）とを備える他、第１又は第３の実施形態の文書認証システム１０１と同様に構成されている。

【０１９８】なお、甲システム１０１ａと乙システム１０１ｂは上記説明したそれぞれの各機能を組み合わせ、同一の処理が実行できるシステムとしてもよい。

【０１９９】また、外部認証システム１０２は、見出し付き認証データ７に代えて見出し付き認証データ３６について図４と同様な処理を施すように構成され、さらに見出し付き暗号データを乙システム１０１ｂでなく甲システム１０１ａに送信する他、第１又は第３の実施形態と同様に構成されている。すなわち、見出し付き認証データ３６は図４の見出し付き認証データ７、暗号データ３６Ｄは図４の暗号データ７Ｄ、外部認証データ３６Ａは図４の外部認証データ７Ａ、見出し３６Ｈは図４の見出し７Ｈに対応する。また、見出し付き暗号データ３９は図４の合成データ１０、見出し３９Ｈは図４の見出し

１０Ｈ、暗号データ３９Ｄは図４の暗号データ１０Ｄに対応する。さらに、暗号化手段３８は図４の暗号化手段９に対応し、秘密鍵３７は図４の秘密鍵８に対応する。なお、暗号データ３６Ｄは、甲と乙のそれぞれにより暗号化された甲乙の認証データであり、暗号データ３９はこの甲乙の認証データにさらに外部認証が与えられて暗号化されたものである。

【０２００】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図１３及び図１４を用いて説明する。

【０２０１】図１４は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【０２０２】まず、甲システム１０１ａにおいて、外部記憶装置１１４、ハードディスク装置１２８から、あるいはネットワーク１００を介して電子文書１が読み込まれる（Ｗ１）。次に電子文書１から見出し部分が取出され、金額情報と印紙税支払者名が記入され、その他必要事項を編集して見出し３Ｈとする（Ｗ２）。

【０２０３】次に、電子文書１から特徴抽出手段２によって特徴データ３Ｄが抽出される（Ｗ３）。さらに特徴データ３Ｄが契約者甲の秘密鍵４（甲）を用いて暗号化手段５によって暗号化され暗号データ６Ｄが生成される（Ｗ４）。見出し３Ｈ（６Ｈ）と暗号データ６Ｄとが結合され契約者甲の電子署名データである見出し付き暗号データ６が生成される（Ｗ５）。

【０２０４】この契約者甲の電子署名データは甲システム１０１ａから契約者乙の使用する乙システム１０１ｂに電子文書１と共に送信される（Ｗ６）。なお、乙に電子文書１を送信するのは、乙が認証するに当たりその文書内容を確認できるようにするためである。

【０２０５】乙システム１０１ｂにおいては、まず、契約者甲の電子署名（見出し付き暗号データ６）と電子文書１が受信される（Ｗ７）。この受け取った電子署名データが見出し３２Ｈと暗号データ３２Ｄとに分離される（Ｗ８）。

【０２０６】次に、暗号データ３２Ｄに乙の認証データ３２Ａが結合されて結合データが生成される（Ｗ９）。この認証データ３２Ａには乙の名前と日付が含まれる。次に暗号データ３２Ｄと認証データ３２Ａが乙の秘密鍵３３を用いて暗号化手段３４によって暗号化され、暗号データ３５Ｄが生成される（Ｗ１０）。

【０２０７】そして、見出し３２Ｈ（３５Ｈ）と暗号データ３５Ｄとが結合されることで甲と乙の電子署名３５（見出し付き暗号データ３５）となる（Ｗ１１）。この電子署名３５は甲の秘密鍵４（甲）で暗号化された部分と乙の秘密鍵３３（乙）で暗号化された部分が含まれ、更に見出し６Ｈ及び認証データ３２Ａに甲乙の名前が含まれるため、実質的に両者の電子署名となるものである。また、見出し３５Ｈあるいは暗号データ３５Ｄに甲乙の正規の電子署名を含ませるようにしてもよい。

【０２０８】こうして生成された甲と乙の電子署名３５は外部認証機関９９の外部認証システム１０２にネットワーク１００を介して送信される（Ｗ１２）。

【０２０９】外部認証システム１０２においては、甲と乙の電子署名３５が受信される（Ｗ１３）。次に、甲と乙の電子署名３５が見出し３６Ｈと暗号データ３６Ｄとに分離される（Ｗ１４）。さらに暗号データ３６Ｄに外部認証機関の外部認証データ３６Ａが結合される（Ｗ１５）。外部認証データ３６Ａには外部認証機関９９の名前と日付および印紙税支払い済の記事が含まれる。印紙税の支払については、予め甲が外部認証機関９９との間で契約をしておく。

【０２１０】次に、暗号データ３６Ｄと認証データ３６Ａとが外部認証機関９９の秘密鍵３７を用いた暗号化手段３８によって暗号化され、暗号データ３９Ｄが生成される（Ｗ１６）。さらに、見出し３６Ｈ（３９Ｈ）と暗号データ３９Ｄが結合され甲乙及び外部認証機関９９の電子署名である見出し付き暗号データ３９が完成する（Ｗ１７）。この電子署名がネットワーク経由で甲システム１０１ａに送信される（Ｗ１８）。

【０２１１】甲システム１０１ａにおいては、電子署名である見出し付き暗号データ３９を見出し付き暗号データ４０として受け取る（Ｗ１９）。そして、この電子署名である見出し付き暗号データ４０が電子文書１と合成されて電子契約書４１（認証付き電子文書４１）が完成する。

【０２１２】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、甲と乙と外部認証機関９９とでそれぞれ電子文書１について認証を与え、かつそれぞれの秘密鍵で認証データを暗号化するようにしたので、作成された電子契約書に対する改竄を防止することができ、かつこれを証拠能力のある電子文書とすることができる。

【０２１３】つまり、電子契約書の改竄を行うとその電子文書１の有する特徴データが変化すること、最初に抽出された特徴データ３Ｄが契約者の甲乙および外部認証機関の全員で暗号化されている事によって電子契約書の改竄を行うと必ず発見できる事から、紙の代わりに電子文書での契約が可能になるものである。さらに、従来の紙の文書では改竄の有無を判定するには高度な技術が必要とされたが、本発明になる電屍文書の改竄防止システムでは容易に改竄の有無を証明できる。また、電子化により保管場所が削減されると共に遠隔地への電送が瞬時に行えるようになり、コンピュータによる検索が行えるようになる。

【０２１４】加えて紙の契約書では字句の誤りを訂正する為に捨て印を押す悪習が有ったが、電子化により、契約者間で瞬時に文書のやり取りが可能になるので、捨て印を押さなくても直ちに訂正して再署名が可能と成り、契約者間のトラブルの発生を防止できる。電子署名３５

に契約金額、印紙税支払者名が記載されているので、外部認証機関に電子文書そのものを送る必要が無く、秘密としたい事項が有る場合でも電子契約書を使用できる。

【０２１５】また、本実施形態では、電子文書１から特徴データを取り出して、これに甲乙、外部認証機関の認証を与えるようにしたが、本発明はこのような場合に限られるものでない。例えば元の電子文書１自体に文書作成者の関係者や上司が上司印等に相当するデータを付加し、当該上司印が付加された電子文書１から特徴データ３Ｄを取り出すようにすれば、実質的にその上司の認証をも付与された電子文書１を取り出すことが可能となる。元の電子文書を改竄すれば特徴データが変化するからである。

【０２１６】さらに、例えば本実施形態では、契約者が甲と乙の２人である場合を説明したが、本発明はこのような場合に限られるものではない。例えば契約者が甲、乙、丙の３者になる場合には、図１３での乙のステップが丙に付いても繰り返し行われるようにすれば３人が契約者の認証が入った上記と同様な電子契約書を作成することができる。また、契約者に更に丁がいる場合には丁に付いてもこの乙のステップを繰り返し行えばよい。従って、契約者の人数には、かかわらず電子契約書を作成し使用できることとなる。

【０２１７】（第６の実施の形態）本実施形態では第５の実施形態で作成した電子契約書が真正なものであることを確認し、また契約者や外部認証機関の付した各認証日付等の認証情報を取り出すシステムについて説明する。

【０２１８】図１５は本発明の第６の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図４、図７、図９、図１１及び図１３と同一部分には同一符号を付し、その説明を省略する。また、本実施形態のシステムには、図６に示す認証文書認証システム１０３が用いられており、本実施形態の独自な機能部分は、認証文書確認プログラム１３５に修正が加えられたことによるものである。

【０２１９】この電子文書の改竄防止システムは、図１に示した認証文書確認システム１０３として構成されるものであり、電子契約書の照合システムでもある。

【０２２０】認証文書確認システム１０３は、電子契約書４１（認証付き電子文書４１）に付された見出し付き暗号データ４０に対し、外部認証機関９９の公開鍵４２（認）、契約者乙の公開鍵４５（乙）及び契約者甲の公開鍵４８（甲）による復号を行い、外部認証機関の認証事実及び認証日付、乙の認証事実及び認証日付を取り出して認証確認を行うとともに、特徴データ５０を取出し、一方、見出し付き暗号データ４０を取り除いた電子文書１から特徴データ５２を取出し、両特徴データ５０，５２を照合して同一性判定を行うようになっている。

【０２２１】このために電子文書の改竄防止システムには、電子契約書４１から見出し付き暗号化データ４０を取り出す手段（図示せず）と、これに含まれる暗号データ４０Ｄを外部認証機関の公開鍵４２（認）で復号する復号化手段４３と、復号化手段４３により復号化された外部認証データ４４Ａから外部認証機関の認証事実と認証日付を日付認証４４Ａ－Ｄとして取り出す手段（図示せず）と、復号化手段４３により復号化された暗号データ４４Ｄを乙の公開鍵４５（乙）で復号化する復号化手段４６とが設けられている。さらに、復号化手段４６により復号化された乙の認証データ４７Ａから乙の認証事実と認証日付を日付認証４７Ａ－Ｄとして取り出す手段（図示せず）と、復号化手段４６により復号化された暗号データ４７Ｄを甲の公開鍵４８（甲）で復号化する復号化手段４９とが設けられている。一方、電子契約書４１から見出し付き暗号化データ４０が除かれた元の電子文書１から特徴抽出を行って特徴データ５２を生成する特徴抽出手段５１と、この特徴データ５２と復号化手段４９により復号化された特徴データ５０Ｄとを照合して電子文書の同一性判定５３－Ｊを行う照合手段５３とが設けられている。

【０２２２】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図１５を用いて説明する。

【０２２３】まず、外部記憶装置１１４、ハードディスク装置１２８から、あるいはネットワーク１００を介して電子契約書４１が読み込まれ、認証データである見出し付き暗号データ４０が取出される。この見出し付き暗号データ４０から暗号データ４０Ｄが取出され、外部認証機関の公開鍵４２を用いて復号化手段４３により復号化され暗号データ４４Ｄと認証データ４４Ａが生成される。暗号データ４４Ｄは図１３の暗号データ３６Ｄに対応するもので、外部認証データ４４Ａは図１３の外部認証データ３６Ａに対応するものである。

【０２２４】外部認証データ４４Ａからは日付認証４４Ａ－Ｄが取出される。暗号データ４４Ｄは契約者乙の公開鍵４５を用いて復号化手段４６によって復号化され、暗号データ４７Ｄと認証データ４７Ａとが取出される。暗号データ４７Ｄは図１３の暗号データ３２Ｄに対応し、認証データ４７Ａは図１３の乙の認証データ３２Ａに対応する。

【０２２５】認証データ４７Ａからは乙の日付認証４７Ａ－Ｄが取出される。暗号データ４７Ｄは契約者甲の公開鍵４８を用いて復号化手段４９によって復号化され特徴データ５０Ｄが取出される。

【０２２６】一方電子文書４１から認証データ４０を取り除いたデータは電子文書１のデータに相当する。電子文書１に相当するデータから特徴抽出手段５１によって特徴を抽出して特徴データ５２が得られる。

【０２２７】照合手段５３で特徴データ５０Ｄと特徴デ

ータ５２とが比較照合され、同一性判定５３－Ｊが得られる。同一性判定５３－Ｊが同一を示していれば電子文書の改竄は行われていないが、そうでない時には改竄が行われている。

【０２２８】また、甲作成の電子文書１に対する外部認証機関及び乙の認証事実と、認証日付が表示されることになり、契約書についての正当性が確認される。

【０２２９】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、特徴データ５０Ｄ，５２による同一性判定及び甲作成の電子文書１に対する外部認証機関及び乙の認証事実並びに認証日付が確認されるので、電子契約書の同一性の判定を効果的に行う事ができ、裁判の場で文書の正当性が証明できるようになる。

【０２３０】なお、本実施形態では、契約者が甲と乙の２者の場合を説明したが、本発明はこの場合に限られるものではない。契約者が、甲、乙、丙の３者になる場合には図１５での乙のステップが丙に付いても繰り返し行われるだけでよい。さらに契約者に更に丁がいる場合は丁に付いても乙のステップを繰り返し行えばよい。従って、契約者の人数にはかかわらない、複数人の間でかわされた電子契約書を確認することができる。

【０２３１】（第７の実施の形態）本実施形態は、上記各実施形態における例えば図４や図７の見出し１１Ｈの編集手段の具体的な例を説明するとともに、認証付き電子文書１２を表示あるいは印刷させるときの表示編集手段について説明する。

【０２３２】図１６は本発明の第７の実施形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図４、図７、図９、図１１、図１３及び図１５と同一部分には同一符号を付し、その説明を省略する。本実施形態のシステムには、図２に示す文書認証システム１０１、あるいは図６に示す認証文書確認システム１０３が用いられている。本実施形態の独自な機能部分は、文書認証プログラム１３３あるいは認証文書確認プログラム１３５に修正が加えられたことによるものである。

【０２３３】この電子文書の改竄防止システムは、図１に示す文書認証システム１０１、あるいは認証文書確認システム１０３に以下に説明する手段が付加されてなる。なお、以下、文書認証システム１０１の場合を例にとって説明する。

【0.２３４】本実施形態の文書認証システム１０１では、第１、第３、第５実施形態と同様な構成の他、表示印刷手段を備え、また、見出しの編集手段が具体的に示される。

【０２３５】見出しの編集手段には、見出し１１Ｈを編集する際に、印鑑等が押された表示物をイメージ情報である印影５４として取り込むスキャナ１１５（図２等）と、この印影５４を電子印鑑６０の一部に加える手段

（図示せず）と、印影５４から特徴抽出して特徴データを生成する特徴抽出手段５５と、特徴データ５６を秘密鍵４で暗号化する暗号化手段５８と、暗号化された暗号化印影５９を電子印鑑６０の一部に加える手段（図示せず）と、電子印鑑６０に名前等を加える入力手段（入力装置１１２）と、完成した電子印鑑６０を見出し１１Ｈ（３Ｈ）として見出し付き特徴データ３（図１６では合成データ１１）に加える手段（図示せず）とが設けられている。なお、電子印鑑６０は、印影５４と暗号化印影５９と所有者の名前を合成してなるものである。

【０２３６】一方、表示印刷手段には、合成データ１１の見出し１１Ｈから日付・署名・印影情報６１を取り出す手段（図示せず）と、これらのデータを表示領域内に収まるように整形する手段６２と、一方、認証付き電子文書１２から電子文書１をと取り出す手段（図示せず）と、取り出された電子文書１の中に記載されるタグ及び表示領域情報１Ｔに整形された日付・署名・印影情報を重ね合わせる手段（図示せず）と、この重ね合わされた表示文書６３を印刷あるいは表示する手段（表示装置１１１、印刷装置１１３）とが設けられている。

【０２３７】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図１６、図１７、図１８及び図１９を用いて説明する。

【０２３８】まず電子印鑑６０を生成する処理を図１６および図１７により説明する。

【０２３９】図１７は本実施形態の電子文書の改竄防止システムの電子印鑑生成処理を示す流れ図である。

【０２４０】まず、電子印鑑の所有者名が入力装置１１２により入力される（Ｘ１）。次に印影データ５４が読込まれる（Ｘ２）。印影データは紙に印鑑を押したものをスキャナ１１５で読み取り電子化したものが用いられる。

【０２４１】次に、印影データ５４から特徴抽出手段５５で特徴が抽出され特徴データ５６が生成される（Ｘ３）。特徴データ５６が所有者の秘密鍵４を使用した暗号化手段５８により暗号化され暗号化印影５９が生成される（Ｘ４）。印影データ５４、暗号化印影５９及びステップＸ１で入力した所有者名が一つのデータとして纏められ電子印鑑６０が生成される（Ｘ５）。そして、電子印鑑６０が第１の実施の形態の図１の見出しデータ３Ｈに入れられる。この結果図１６の認証付き電子文書１２の見出し１１Ｈに電子印鑑６０のデータが保存されることとなる（Ｘ６）。

【０２４２】次に改竄を防止した電子印鑑の照合処理を図１８により説明する。

【０２４３】図１８は本実施形態の電子文書の改竄防止システムの電子印鑑照合処理を示す流れ図である。

【０２４４】この照合処理は、電子文書１自体の同一性判定と別途に行われるものであり、見出し１１Ｈに含ま

れる電子印鑑（電子署名）の正当性を評価するものである。なお、この処理の手段は特に図１６では示していないが、その手段は文書認証プログラム１３３あるいは認証文書確認プログラム１３５とシステムのハードウエアで実現されるものであり、図１８で示される処理を実現するものである。

【０２４５】まず、所有者名が入力される（Ｙ１）。所有者名に従いその所有者の公開鍵が外部記憶装置１１４、ハードディスク装置１２８から、あるいはネットワーク１００を介して読込まれる（Ｙ２）。次に、電子印鑑６０の中にある暗号化印影が公開鍵を用いて復号化される（Ｙ３）。

【０２４６】一方、電子印鑑６０の中にある印影データから特徴抽出が行われる（Ｙ４）。次に、ステップＹ３で復号化した特徴データとステップＹ４で抽出した特徴データとの照合が行われる（Ｙ５）。

【０２４７】この照合結果の判定が行われ（Ｙ６）、印鑑が不一致であれば表示装置１１１にその旨表示される。一方、印鑑が一致していればその旨が表示される。

【０２４８】次に電子文書に電子印鑑や日付を重ね合わせて表示または印刷できるように、文書及び見出しを編集する処理を図１６および図１９により説明する。

【０２４９】図１９は本実施形態の電子文書の改竄防止システムの文書見出し編集処理を示す流れ図である。

【０２５０】まず、電子文書１の編集が行われる（Ｚ１）。この処理は電子文書１そのものの作成作業でありシステム使用者による作業である。さらに電子文書１にシステム使用者による作業で表示領域が設定される（Ｚ２）。この段階で日付・署名・印影情報を表示する場所が決められる。

【０２５１】次に電子文書１の内部にステップＺ２作成した表示領域にタグおよび表示領域情報１Ｔを埋め込む（Ｚ３）。

【０２５２】ここから見出し編集に入り、日付・署名・印影情報６１が編集される（Ｚ４）。さらに見出しデータ１１Ｈに埋め込むタイトル情報が入力されるか、もしくは電子文書内のタイトル部分が指定されその値が見出し１１Ｈに取り込まれる（Ｚ５）。そして見出し１１Ｈが保存される（Ｚ６）。

【０２５３】次に、電子文書１が保存される（Ｚ７）。なお、電子文書１には見出し１１Ｈ自体が埋め込まれる訳ではないので、ステップＺ３の電子文書１へのタグおよび表示領域情報１Ｔ埋め込みの後に直ちにステップＸ７の文書保存を行ってもよい。

【０２５４】以上の処理により、電子文書１のどの場合に日付・署名・印影情報６１を表示したらよいかが記録されるので、電子文書１を表示または印刷する時には、図１６で示したように、電子文書上に日付・署名・印影を重ね合わせて表示文書６３とすることができる。

【０２５５】これにより、改竄を防止した電子文書１２に改竄を防止した電子印鑑６０が付けられ、さらにこれらを重ね合わせた表示文書６３として、表示または印刷されることになる。

【０２５６】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、特徴抽出を行って暗号化した電子印鑑６０を見出し３Ｈに加えるようにしたので、電子印鑑６０の印影改竄の有無が判定でき、電子文書に改竄を防止した印影を張り付けることができる。

【０２５７】また、このように改竄を防止した印影を、改竄を防止しまた改竄の有無判定ができる電子文書と合わせて、表示や印刷ができるようにしたので、この改竄防止が保障された表示や印刷によって、従来の紙の文書と同様な運用が可能となる。従来の紙の文書と同じ運用が可能でありながら、伝送で文書を瞬時に遠隔地に送る事ができる為その効果は非常に大である。なお、この場合、表示文書６３に表示される電子文書は、同一性判定及び認証確認を行ったものを用いればより効果的である。

【０２５８】なお、本実施形態では、１つの電子印鑑６０を見出し３Ｈに入れる場合で説明したが、本発明はこれに限られるものではない。見出しデータは編集する事が可能である為、図４や図７における使用の外に、図１３や図１５の使用においても運用する事ができ、電子文書の中に甲の日付・署名・印影と乙の日付・署名・印影を入れる事ができる。この場合にも電子文書１そのものは改竄される事が無い事は言うまでもない。

【０２５９】さらに、以上の説明では紙に印鑑を押したものをスキャナ１１５で読取り電子化した印影を用いるとしたが、紙に手書きのサインをしてスキャナ１１５で読取り電子化した電子サインを用いてもよい。

【０２６０】（第８の実施の形態）本実施形態は、上記第１～第７の実施形態で使用される特徴抽出手段の構成動作の例を説明する。

【０２６１】図２０は本発明の第８の実施の形態の電子文書の改竄防止システムにおける特徴抽出方法を説明するための図である。

【０２６２】また、図２１は本実施形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図４、図７、図９、図１１、図１３、図１５及び図１６と同一部分には同一符号を付し、その説明を省略する。また、本実施形態のシステムには、図２に示す文書認証システム１０１、あるいは図６に示す認証文書認証システム１０３が用いられている。本実施形態の独自な機能部分は、文書認証プログラム１３３あるいは認証文書確認プログラム１３５に修正が加えられたことによるものである。

【０２６３】この電子文書の改竄防止システムは、図１に示す文書認証システム１０１、あるいは認証文書確認システム１０３における特徴抽出手段として以下に説明

する手段が設けられて構成される。なお、以下、文書認証システム１０１の場合を例にとって説明する。

【０２６４】図２１に示すように、文書認証システム１０１又は認証文書確認システム１０３の特徴抽出手段２（２０，５１，５５）は、電子文書１から特徴データ３Ｄを生成する。

【０２６５】この特徴抽出手段２には、データＳ＿ｓｕｍを格納する部分とデータＩＳ＿ｓｕｍを格納する２５６個の配列と、図示しない処理手段とが設けられている。この処理手段は以下に説明する処理を実現する機能実現手段である。

【０２６６】まず、図２０は特徴抽出手段のデータの流れを示している。

【０２６７】同図において、電子文書やファイル等のデータそのもの，すなわちＳｔｒｅａｍは、電子文書データ並びＳをなしている。この電子文書データ並びＳは、２５６バイトずつに区切られた電子文書データ並び部分Ｓ１、Ｓ２、Ｓ３、．．、Ｓｎにより構成される。

【０２６８】このＳｔｒｅａｍから生成されるＳ＿ｓｕｍ＿ｓｔｒｅａｍは、合計データ並びＳ＿ｓ＿ｓｔｒｅａｍをなしている。この合計データ並びＳ＿ｓ＿ｓｔｒｅａｍは、合計データ並び部分ＳＳ１、ＳＳ２、ＳＳ３、．．から構成される。ＳＳ１は、Ｓ１、Ｓ２、Ｓ３、．．、Ｓ２５６それぞれの合計値を２５６個のデータの並びとしたものである。同様に、ＳＳ２は、Ｓ２５７～Ｓ５１２それぞれの合計値をデータの並びとしている。

【０２６９】一方、ＳｔｒｅａｍからはＩｎｔｅｒｖａｌｅｄ　Ｓｔｒｉｎｇとして間隔を置いたデータ並びＩＳが生成される。この間隔を置いたデータ並びＩＳは間隔を置いたデータ並び部分ＩＳ１、ＩＳ２、ＩＳ３、．．、ＩＳｎから構成される。ここで、ＩＳ１は、Ｓ１、Ｓ２、Ｓ３、．．、Ｓ２５６の各先頭データを順次２５６個並べたものであり、ＩＳ２は、Ｓ１、Ｓ２、Ｓ３、．．、Ｓ２５６の各２番目のデータを順次２５６個並べたものである。以下同様に、ＩＳ３～ＩＳ２５６が構成される。ＩＳ２５７は、Ｓ２５７～Ｓ５１２の各先頭データを順次２５６個並べたものである。以下同様である。

【０２７０】このＩｎｔｅｒｖａｌｅｄ　Ｓｔｒｉｎｇから生成されるＩＳ＿ｓｕｍ＿ｓｔｒｅａｍは、間隔を置いた合計データ並びＩＳ＿ｓ＿ｓｔｒｅａｍをなしている。この間隔を置いた合計データ並びＩＳ＿ｓ＿ｓｔｒｅａｍは、間隔を置いた合計データ並び部分ＩＳＳ１、ＩＳＳ２、ＩＳＳ３、．．から構成される。この間隔を置いた合計データ並び部分ＩＳＳ１、ＩＳＳ２、ＩＳＳ３、．．は、間隔を置いたデータ並び部分ＩＳ１～ＩＳｎから生成され、その生成方法は、Ｓ１～ＳｎからＳＳ１、ＳＳ２、ＳＳ３、．．を生成する方法と同じである。

【０２７１】なお、最終的には、合計データ並びＳ＿ｓ＿ｓｔｒｅａｍと間隔を置いた合計データ並びＩＳ＿ｓ＿ｓｔｒｅａｍとが特徴データ３Ｄとなる。

【０２７２】ここで、図２０と図２１との関係を説明すると以下の通りである。

【０２７３】Ｓ１は２５６バイトのデータの並びで、このＳ１のデータの合計値が図２１のＳ＿ｓｕｍに格納され、Ｓ＿ｓｕｍの値がＳ＿ｓ＿ｓｔｒｅｍに出力される。Ｓ＿ｓ＿ｓｔｒｅｍはワード（１６ビット）のデータの並びで２５６バイトの合計値を取っても桁落ちは発生しない。同様にＳ１に続くデータの並びＳ２に対しても合計値がＳ＿ｓ＿ｓｔｅｒａｍに出力される。以下、Ｓ３からＳｎに至るまで同様に行われる。

【０２７４】ＩＳ１は２５６バイトのデータの並びでＳ１の先頭１バイト、Ｓ２の先頭１バイトＳ３のい先頭１バイトと続き、Ｓ２５６の先頭１バイトまでが格納される。ＩＳ２は同様に２５６バイトのデータの並びでＳ１の２バイト目、Ｓ２の２バイト目、Ｓ３の２バイト目と続き、Ｓ２５６の２バイト目までが格納される。同様にＩＳ３は同様に２５６バイトのデータの並びでＳ１の３バイト目、Ｓ２の３バイト目、Ｓ３の３バイト目と続き、Ｓ２５６の３バイト目までが格納される。ＩＳ２５６はＳ１の２５６バイト目、Ｓ２の２５６バイト目、Ｓ３の２５６バイト目と続き、Ｓ２５６の２５６バイト目までが格納される。ＩＳ１からＩＳ２５６までのデータはそれぞれ合計が取られて、図２１のＩＳ＿ｓｕｍ［０］からＩＳ＿ｓｕｍ［２５５］に格納され、ＩＳ＿ｓｕｍの並びがＩＳ＿ｓ＿ｓｔｒｅａｍに出力される。ＩＳ＿ｓ＿ｓｔｒｅａｍはワードのデータの並びで２５６バイトの合計値を取っても桁落ちは発生しない。

【０２７５】こうしてＳ＿ｓ＿ｓｔｒｅａｍとＩＳ＿ｓ＿ｓｔｒｅａｍからなる特徴データが得られるが、次にこの処理のフローを図２２で説明する。

【０２７６】図２２は本実施形態の電子文書の改竄防止システムの特徴データ抽出の処理の一例を示す流れ図である。

【０２７７】まず、全てのデータが初期化される（Ａ１）。次に電子文書データ並びＳのデータが有るかどうかが調べられる（Ａ２）。

【０２７８】データが有る場合にはステップＡ３に移り、Ｓから１バイトが読込まれる。一方、データが無い場合にはステップＡ４に移り終了処理が行われる。

【０２７９】ステップＡ３でＳから１バイトを読んだ後は、読んだ値がＳ＿ｓｕｍとＩＳ＿ｓｕｍ［ｉ］に加算される（Ａ５）。

【０２８０】次に、ｉが２５５かどうかが調べられる（Ａ６）。ｉが２５５でない場合にはｉを１増加させ（Ａ７）、ステップＡ２に戻る。一方、ｉが２５５の場合には（Ａ６）、Ｓ＿ｓｕｍの値がＳ＿ｓ＿ｓｔｒｅａｍに出力されｉがゼロに戻される（Ａ８）。

【０２８１】次に、ｊが２５５かどうかが調べられる（Ａ９）。ｊが２５５でない場合にはｊを１増加させ（Ａ１０）、ステップＡ２に戻る。一方、ｊが２５５の場合には（Ａ９）、ＩＳ＿ｓｕｍ［１］からＩＳ＿ｓｕｍ［２５５］までの値をＩＳ＿ｓ＿ｓｔｒｅａｍに出力してｊをゼロに戻し（Ａ１１）、ステップ２に戻る。

【０２８２】このような処理により、電子文書のデータが１バイトづつ順次読込まれ、全データが処理されるまで図２０のデータ（Ｓ＿ｓ＿ｓｔｒｅａｍ，ＩＳ＿ｓ＿ｓｔｒｅａｍ）が生成されつづけ、特徴データ３Ｄとして出力される。

【０２８３】このＳ＿ｓ＿ｓｔｒｅａｍ及びＩＳ＿ｓ＿ｓｔｒｅａｍを特徴データとした場合、電子文書データ並びＳ（電子文書１や印影５４等）のどの１バイトの値が変化してもＳ＿ｓ＿ｓｔｒｅａｍの何処かの１ワードが変化する。また、電子文書データ並びＳのどの２バイトを入れ替えてもＩＳ＿ｓ＿ｓｔｒｅａｍの何処かの１ワードが変化する。

【０２８４】例えば、Ｓ１のデータ部分内部でデータの入れ替えを行うと、Ｓ１の合計値は変化しないがＩＳ＿ｓｕｍ［０］からＩＳ＿ｓｕｍ［２５５］の何処かの値は必ず変化する。これによって電子文書１のどのデータを改竄しても改竄の事実が発見される。また、Ｓ１の２５６バイトのデータが１ワードに圧縮され、ＩＳ１の２５６バイトのデータが１ワードに圧縮される事から、元のデータの１／６４のサイズにデータが圧縮される。また、このように生成される特徴データは、データの圧縮が一方向性であり、特徴データから元のデータを再現する事はできない。

【０２８５】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、特徴抽出手段により、図２０に示すようなＳ＿ｓ＿ｓｔｒｅａｍ及びＩＳ＿ｓ＿ｓｔｒｅａｍを特徴データとして生成するようにしたので、元のデータのどの部分がどの様に変化してもその変化を発見することができる。また、特徴データは元のデータに比較してデータサイズが大幅に小さくなり取り扱いが容易である。また、特徴データの取出し方がシンプルで演算を高速にすることができる。

【０２８６】さらに、特徴データから元のデータを再現できない事から、外部認証機関９９に電子文書１を開示したくない場合には、認証対象を不開示のまま電子文書の認証を行うことができる。特徴データを用いる方法では電子文書の認証にその文書自体の引き渡しが必要ないからである。

【０２８７】（第９の実施の形態）本実施形態は、上記第１～第７の実施形態で使用される特徴抽出手段の構成動作の他の例を説明する。

【０２８８】図２３は本発明の第９の実施の形態の電子文書の改竄防止システムにおける特徴抽出方法を説明するための図であり、図２０と同一部分には同一符号を付してその説明を省略する。

【０２８９】また、本実施形態の電子文書の改竄防止システムには、図２に示す文書認証システム１０１、あるいは図６に示す認証文書認証システム１０３が用いられ、特徴抽出手段として以下に説明する手段が設けられている。なお、本実施形態の独自な機能部分は、文書認証プログラム１３３あるいは認証文書確認プログラム１３５に修正が加えられたことによるものである。

【０２９０】本実施形態における特徴抽出は、Ｓ＿ｓ＿ｓｔｒｅａｍ及びＩＳ＿ｓ＿ｓｔｒｅａｍが抽出されるまでは第８の実施形態と同様に行われる。また、Ｓ＿ｓ＿ｓｔｒｅａｍからＳ＿ｓ＿ｓｔｒｅａｍ′、ＩＳ＿ｓ＿ｓｔｒｅａｍからＩＳ＿ｓ＿ｓｔｒｅａｍ′が生成され、これらのＳ＿ｓ＿ｓｔｒｅａｍ′及びＩＳ＿ｓ＿ｓｔｒｅａｍ′が最終的な特徴データ３Ｄとして使用される。なお、Ｓ＿ｓ＿ｓｔｒｅａｍ′及びＩＳ＿ｓ＿ｓｔｒｅａｍ′はロングワード（３２ビット）で構成される。

【０２９１】具体的な処理としては以下のようになる。

【０２９２】まず、ＳＳ１等とＩＳＳ１等を生成する手前までは第８の実施形態と同様である。第８の実施の形態では実際の処理においてはＳＳ１等とＩＳＳ１等を２５６ワード単位で区切らずにＳ＿ｓ＿ｓｔｒｅａｍ及びＩＳ＿ｓ＿ｓｔｒｅａｍとしてそのまま出力していた。これに対して図２３においてはＳ１、Ｓ２、Ｓ３、．．．、Ｓｎを２５６バイトずつ合計して成る値の列を２５６ワードづつＳＳ１、ＳＳ２…ＳＳ２５６の合計値のロングワードの列にしてＳ＿ｓ＿ｓｔｒｅａｍ′に出力する。また、ＩＳ１、ＩＳ２、ＩＳ３、．．．、ＩＳ２５６の合計値のロングワードの列をＩＳ＿ｓ＿ｓｔｒｅａｍ′に出力する。

【０２９３】いいかえると、Ｓ＿ｓ＿ｓｔｒｅａｍ′には、ＳＳ１、ＳＳ２、．．それぞれの合計値が順次データ並びとして出力され、同様に、ＩＳ＿ｓ＿ｓｔｒｅａｍ′には、ＩＳＳ１、ＩＳＳ２、．．それぞれの合計値が順次データ並びとして出力される。

【０２９４】これによって、図２０ではＳ＿ｓ＿ｓｔｒｅａｍはワードのストリームであったが、図２３ではＳ＿ｓ＿ｓｔｒｅａｍ′はロングワードのストリームとなる。同様に、図２０ではＩＳ＿ｓ＿ｓｔｒｅａｍはワードのストリームであったが、図２３ではＩＳ＿ｓ＿ｓｔｒｅａｍはロングワードのストリームとなる。これによりデータ量は更に１／１２８に圧縮され、最初の１／８１９２の大きさになる。

【０２９５】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、特徴抽出手段により、図２３に示すようなＳ＿ｓ＿ｓｔｒｅａｍ′及びＩＳ＿ｓ＿ｓｔｒｅａｍ′を特徴データとして生成するようにしたので、第８の実施形態と同様な効果が得られる他、第８の実施形態の場合よりも更に特徴データ

をコンパクトなものとすることができる。

【０２９６】なお、第９の実施形態では第８の実施形態に対してデータの２５６個毎の合計を１回余分に行っているが、１回だけでは無く更に繰り返してデータを圧縮してもよい。このようにすればより一層特徴データをコンパクトなものとすることができる。

【０２９７】（第１０の実施の形態）本実施形態は、上記第１～第７の実施形態で使用される特徴抽出手段の構成動作のさらに他の例を説明する。

【０２９８】図２４は本発明の第１０の実施の形態の電子文書の改竄防止システムにおける特徴抽出方法を説明するための図である。

【０２９９】また、図２５は本実施形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図４、図７、図９、図１１、図１３、図１５及び図１６と同一部分には同一符号を付し、その説明を省略する。また、本実施形態のシステムには、図２に示す文書認証システム１０１、あるいは図６に示す認証文書認証システム１０３が用いられている。本実施形態の独自な機能部分は、文書認証プログラム１３３あるいは認証文書確認プログラム１３５に修正が加えられたことによるものである。

【０３００】この電子文書の改竄防止システムは、図１に示す文書認証システム１０１、あるいは認証文書確認システム１０３における特徴抽出手段として以下に説明する手段が設けられて構成される。なお、以下、文書認証システム１０１の場合を例にとって説明する。

【０３０１】図２５に示すように、文書認証システム１０１又は認証文書確認システム１０３の特徴抽出手段２（２０，５１，５５）は、電子文書１から特徴データ３Ｄを生成する。

【０３０２】特徴抽出手段２には、セパレータテーブル２Ｔ及び単語配列２Ｗが設けられている。

【０３０３】一方、図２４において、電子文書１は単語とセパレータの並びで構成される。セパレータというのは、文書中において空白や句読点等の単語を分離するものである。単語配列２Ｗは単語のデータの並びとその順番で構成される。一方、特徴データ３Ｄは単語配列２Ｗのデータ並びの順番データの並びで構成される。

【０３０４】また、セパレータテーブル２Ｔは、予めセパレータとして使用するものを登録したものである。一方、単語配列２Ｗは、単語を格納する領域と配列の順番からなっている。

【０３０５】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムにおける特徴抽出処理について説明する。

【０３０６】まず、図２４で示すように、単語とセパレータから構成された電子文書１の先頭から順次データが読み込みまれ、セパレータとセパレータで区切られたデータが単語とみなされる。見つけた単語のうち新しいものが単語配列２Ｗに登録され、その単語の配列番号が特徴データ３Ｄに書き出される。すなわちこの配列番号の並びそのものが特徴データとなる。

【０３０７】つまり、特徴抽出手段２により読み込まれた１文字がセパレータテーブル２Ｔのデータと比較され、セパレータでなければ次の１文字が読込まれる。順次読込みが行われ、読み込みを続けて得られた文字列が単語として検出される。この場合に、当該文字列が新しい単語であるか否かが判定される。そして新しい単語の場合には文字配列２Ｗに登録し登録番号を特徴データ３Ｄとして書き出す。既に出てきた単語の場合にはその登録番号を特徴データ３Ｄに書き出す。

【０３０８】この処理を図２６を用いてより具体的に説明する。

【０３０９】図２６は本実施形態の電子文書の改竄防止システムの特徴データ抽出の処理の一例を示す流れ図である。

【０３１０】まず、全てのデータが初期化される（Ｂ１）。次に、電子文書１のデータがあるかどうか調べられ（Ｂ２）、データがある場合には１文字分が読込まれる（Ｂ３）。データが無い場合には（Ｂ２）終了処理が行われる（Ｂ４）。

【０３１１】次に、読込んだ１文字がセパレータかどうかがセパレータテーブル２Ｔのデータとの比較により行われる（Ｂ５）。読込んだ１文字がセパレータの場合には（Ｂ５）、セパレータテーブル２Ｔとセパレータの比較が行われる（Ｂ６）。一方、読込んだ１文字がセパレータでない場合には（Ｂ５）、その文字をバッファに入れてステップＢ２に戻る（Ｂ７）。

【０３１２】ステップＢ６の後、配列２Ｗのテーブルデータ（ハッシュテーブル）とバッファデータの比較が行われる（Ｂ８）。なお、ステップＢ６はセパレータ自体の種類を決定するものであり、ステップＢ８はバッファの中に構成された単語の種類を決定するものである。

【０３１３】次に、ステップＢ６の結果よりテーブルデータ（配列２Ｗ）とセパレータが同じでない場合には（Ｂ９）、データがテーブル２Ｗに登録され（Ｂ１０）ステップＢ１１に移る。一方、同じ場合には（Ｂ９）、ステップＢ１０を行わずにステップＢ１１に移る。

【０３１４】ステップＢ１１では、テーブルデータ（配列２Ｗ）とバッファデータが同じでない場合には、バッファデータがハッシュテーブル２Ｗに登録され（Ｂ１２）、ステップＢ１３に移動する。一方、同じ場合には（Ｂ１１）ステップＢ１２を行わずにステップＢ１３に移動する。

【０３１５】そして、ステップＢ１３では、特徴データ３Ｄにステップ９～Ｂ１２で決定されたセパレータと単語それぞれのテーブル番号が出力される。その後ステップＢ２に戻る。

【０３１６】以上により電子文書１の特徴がハッシュテ

ーブルのテーブル番号並びとして抽出され特徴データ３Ｄとして得られる。

【０３１７】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、特徴抽出手段により単語とセパレータのテーブル番号の並びを特徴データとして抽出するようにしたので、元のデータのどの部分がどの様に変化してもその変化を発見することができる。また、元のデータに比較してデータのサイズが大幅に小さくなり取り扱いが容易である。さらに特徴データから元のデータを再現できない事から、外部認証機関に電子文書を開示したくない場合であっても電子文書の認証を行うことができる。

【０３１８】（第１１の実施の形態）本実施形態は、第１～第７の実施形態で説明した電子文書の改竄防止システムにおける各文書認証システム１０１、外部認証システム１０２及び認証文書確認システム１０３を使用するにあたり、そのシステム使用者を確認するための情報を生成し、また、各システムで用いられる暗号鍵（秘密鍵、公開鍵等）を生成する手段について説明する。

【０３１９】図２７は本発明の第１１の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図４、図７、図９、図１１、図１３、図１５及び図１６と同一部分には同一符号を付し、その説明を省略する。また、本実施形態のシステムには、図２に示す文書認証システム１０１、図３に示す外部認証システム１０２あるいは図６に示す認証文書認証システム１０３が用いられている。本実施形態の独自な機能部分は、文書認証プログラム１３３、外部認証プログラム１３４あるいは認証文書確認プログラム１３５に修正が加えられたことによるものである。

【０３２０】この電子文書の改竄防止システムは、図１に示す文書認証システム１０１、外部認証システム１０２あるいは認証文書確認システム１０３と同様な構成に、以下に各手段が付加されて構成される。なお、以下、文書認証システム１０１の場合を例にとって説明する。

【０３２１】図２７に示す文書認証システム１０１は、システム使用者の指紋を読み取って特徴抽出を行い、この特徴データ６７、別途入力されたパスワード６８及び乱数を用いて暗号鍵７１，７４，７５，７７Ｓ，７７Ｋを生成するとともに、さらに使用者氏名、ＩＤ（識別情報）、パスワード、指紋及び生成した暗号鍵等から本人認証データ７８を生成するものである。この本人認証データ７８は、後述する第１２の実施形態においてシステム使用者を確認するのに用いられる。

【０３２２】この本人認証データ７８を生成するために文書認証システム１０１には、指紋読取り機６４と、イメージデータとして読み取られた指紋６５から特徴データ６７を抽出する特徴抽出手段６６と、入力装置１１２から入力されたパスワード６８及び氏名・ＩＤ６９のうちパスワード６８と特徴データ６７から暗号鍵７１を生成する暗号鍵生成手段７０と、乱数発生器７２と、乱数発生器７２から発生した乱数、パスワード６８及び特徴データ６７から秘密鍵７４及び公開鍵を生成する秘密鍵公開鍵生成手段７３と、暗号鍵７１及び秘密鍵７４から暗号化秘密鍵７７Ｓ及び暗号化暗号鍵７７Ｋを生成する暗号化手段とが設けられている。さらに、文書認証システム１０１には、指紋６５、暗号化秘密鍵７７Ｓ、暗号化暗号鍵７７Ｋ、パスワード６８及び氏名・ＩＤ６９を取り込み、指紋７８Ｆ、暗号化秘密鍵７８Ｓ、暗号化暗号鍵７８Ｋ、パスワード７８Ｐ及び氏名・ＩＤ７８Ｎからなる本人認証データ７８を作成する手段（図示せず）とが設けられている。

【０３２３】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図２７及び図２８を用いて説明する。

【０３２４】図２８は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【０３２５】本動作は文書認証システム１０１のシステム起動時等における本人認証用データを作成する手続きである。

【０３２６】このためにまず、入力装置１１２により、最初に氏名・ＩＤデータ６９とパスワード６８が入力されてシステムが起動される（Ｃ１）。次に、指紋読取り機６４が起動され指紋が読取られる（Ｃ２）。これにより、指紋データ６５が得られる。

【０３２７】次に、指紋データ６５から特徴抽出手段６６によって特徴データ６７が抽出される（Ｃ３）。さらにパスワード６８と特徴データ６７とが使用され暗号鍵生成手段７０により暗号鍵７１が生成される（Ｃ４）。

【０３２８】次に、パスワード６８、乱数発生器７２および特徴データ６７が使用され秘密鍵公開鍵生成手段７３により秘密鍵７４と公開鍵７５が生成される（Ｃ４）。本実施形態では秘密鍵公開鍵生成手段７３としてＲＳＡ方式に対応したものを用いている。なお、ＤＥＳ等を用いてもよい。

【０３２９】次に、暗号鍵７１と秘密鍵７４とが暗号化手段７６により暗号化され暗号化秘密鍵７７Ｓと暗号化暗号鍵７７Ｋが生成される（Ｃ６）。なお、本実施形態では、暗号化手段７６は共通鍵暗号方式の一つであるＤＥＳ方式を用いており、暗号鍵７１をその暗号鍵としている。暗号鍵７１については自分で自分を暗号化する事（暗号化暗号鍵７７Ｋの生成）になる。

【０３３０】そして、指紋データ６５、暗号化秘密鍵７７Ｓ、暗号化暗号鍵７７Ｋ、パスワード６８及び氏名・ＩＤ６９が本人認証データ７８として一つにまとめられ（Ｃ７）、ハードディスク装置１２８等に格納される（Ｃ８）。また、この情報のうち、公開鍵７５は所定の場所に登録されることになる（Ｃ９）。

【０３３１】上述したように、本発明の実施の形態に係

る電子文書の改竄防止システム及び方法は、指紋データを元にして暗号鍵を生成するようにしたので、本人認証を確実なものとすることができるとともに、本人が暗号鍵のデータ自体を知る必要がなく、システムの利用を簡便なものとすることができる。また、暗号鍵そのものが暗号化されていること、秘密鍵が暗号化されている事からたとえ本人認証データ７８を盗まれる事が有っても暗号鍵と秘密鍵の内容を知る事はできず、極めて安全な情報管理を行うことができる。

【０３３２】なお、本実施形態では暗号鍵生成手段７０にパスワードを必要としたが、本発明はこのような場合に限られるものではない。例えば特徴データ６７のみから暗号鍵を生成しても同様の効果が得ることができる。また例えば秘密鍵公開鍵生成手段７３にパスワード６８と乱数発生器７２を必要としていたが、何れか一方が無くても、また両方が無くても同様の効果が得ることが可能である。

【０３３３】さらに、本実施形態では、暗号鍵等の生成に指紋を用いることとしたが、本発明は指紋に限られるものでなく、声紋や虹彩等、本人を特定できるものであれば、種々の生体データを利用することができる。

【０３３４】（第１２の実施の形態）本実施形態は、第１１の実施形態のシステムで登録したシステム使用者に当該システムが使用できるようにする。すなわち、第１～第７の実施形態で説明した電子文書の改竄防止システムにおける各文書認証システム１０１、外部認証システム１０２及び認証文書確認システム１０３を使用するにあたり、そのシステム使用者を確認し、また、各システムで用いられる暗号鍵（秘密鍵、公開鍵等）を使用可能とする手段について説明する。

【０３３５】図２９は本発明の第１２の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図４、図７、図９、図１１、図１３、図１５、図１６及び図２７と同一部分には同一符号を付し、その説明を省略する。また、本実施形態のシステムには、図２に示す文書認証システム１０１、図３に示す外部認証システム１０２あるいは図６に示す認証文書認証システム１０３が用いられている。本実施形態の独自な機能部分は、文書認証プログラム１３３、外部認証プログラム１３４あるいは認証文書確認プログラム１３５に修正が加えられたことによるものである。

【０３３６】この電子文書の改竄防止システムは、図１に示す文書認証システム１０１、外部認証システム１０２あるいは認証文書確認システム１０３と同様な構成に、以下に各手段が付加されて構成される。なお、以下、文書認証システム１０１の場合を例にとって説明する。

【０３３７】図２９に示す文書認証システム１０１は、正当な使用権限を有する者が電子文書の改竄防止システムを使用したい場合に、パスワード６８及び指紋６５を入力させ、これと第１１の実施形態で生成された本人認証データ７８に予め格納された指紋７８Ｆ、パスワード７８Ｐとにより本人確認を行った後、指紋７８Ｆ、パスワード７８Ｐ及び暗号化暗号鍵７８Ｋから暗号鍵を取出し、さらにこの暗号鍵により暗号化秘密鍵７８Ｓを復号して秘密鍵４を取出して、第１～第７の実施形態の電子文書の改竄防止システムを使用可能な状態にする。

【０３３８】このために文書認証システム１０１には、指紋読取り機６４と、読み取られた指紋６５と本人認証データ７８内の指紋７８Ｆとを照合する照合手段８１と、入力装置１１２から入力されたパスワード６８と、本人認証データ７８内のパスワード７８Ｐとを照合する照合手段８０と、照合手段８０及び８１の結果から本人認証の判定を行う判定ロジック手段８２とが設けられている。さらに、文書認証システム１０１には、判定ロジック手段８２から本人が認証された旨を受けると指紋７８Ｆから特徴データ６７を抽出する特徴抽出手段６６と、特徴データ６７及びパスワード７８Ｐから暗号鍵７１を生成する暗号鍵生成手段７０と、暗号化暗号鍵７８Ｋを暗号鍵７１で復号して暗号鍵８４を取り出す復号手段８３と、暗号鍵７１と暗号鍵８４とを照合して正しく暗号鍵７１が取り出されたことを確認する照合手段８５と、取り出された暗号鍵７１を用い暗号化秘密鍵７８から電子文書の改竄防止システム（図４等）で使用する秘密鍵４を取り出す復号手段８６と、氏名・ＩＤ７８Ｎ等を表示する表示手段７９とが設けられている。

【０３３９】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図２９及び図３０を用いて説明する。

【０３４０】図３０は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【０３４１】本動作は生体データ等の入力により本人認証用データに基づいて文書認証システム１０１のシステム起動時等における本人確認及び秘密鍵生成を行う手続きである。

【０３４２】まず、入力装置１１２から本人認証を行う為に名前が入力されると、ハードディスク装置１２８から本人認証データ７８が読み込まれ、表示手段１１１により氏名・ＩＤが表示される。システム使用者は、氏名・ＩＤを確認してパスワード６８を入力する（Ｄ１）。

【０３４３】次に、本人認証データ７８中のパスワード７８Ｐと今入力したパスワード６８とが照合される（Ｄ２）。この照合が一致すれば指紋読み取り機６４で指紋が読取られ、イメージデータである指紋６５が生成される（Ｄ３）。

【０３４４】次に指紋照合手段８１により指紋７８Ｆと読み取った指紋６５とが照合される（Ｄ４）。照合が一致すれば（Ｄ４）、本人認証データ７８から指紋７８Ｆが取り出され特徴抽出手段６６により特徴抽出されて特徴データ６７が生成される（Ｄ５）。ここで読み取った

指紋６５を用いずに本人認証データ７８内の指紋７８Ｆを用いるのは、読み取った指紋６５は１ビットも違わずに指紋７８Ｆと一致することは有り得ず、より取るたびに若干の違いを生じるためである。一方、特徴抽出では第８～第１０の実施形態で説明したようにわずかな違いがあっても異なる特徴データとして抽出されるので、第１１の実施形態で取り出した指紋そのものを使用して暗号鍵７１を取り出そうとするものである。

【０３４５】つまり、この特徴データ６７とパスワード７８Ｐが使用され暗号鍵生成手段７０により暗号鍵７１が生成される（Ｄ６）。次に本人認証データ７８から暗号化暗号鍵７８Ｋが取り出されステップＤ６で生成した暗号鍵７１によって復号される（Ｄ７）。

【０３４６】さらにステップＳＴ７で復号した暗号鍵８４とステップＳＴ６で生成した暗号鍵７１が照合手段８５で照合される（Ｄ８）。照合が一致すれば最終的に本人の認証ができたとみなされる。そして、本人認証データ７８から暗号化秘密鍵７８Ｓが取り出され暗号鍵７１を用いた復号手段８６により復号されて秘密鍵４が生成される（Ｄ９）。

【０３４７】こうして電子文書の改竄防止システムが使用可能になり、文書読取り（Ｄ１０）、特徴抽出（Ｄ１１）、秘密鍵４による特徴データの暗号化（Ｄ１２）等といった各実施形態で説明した処理が行われることとなる。

【０３４８】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、システム使用者の指紋６５を読取り、これと本人認証データ７８とを照合するようにしたので、本人認証データ７８から秘密鍵４を取り出す事ができる。ここで、本人認証データ７８内において秘密鍵と暗号鍵は暗号化されて保存されているので、仮に本人認証データを盗まれても秘密鍵と暗号鍵が知られる事はできず非常に安全である。また、暗号鍵は本人認証データの中に保存された指紋７８Ｆから生成されるので確実に同じ暗号データを再現できると共に、暗号データそのものを誰にも知らせる必要が無く極めて安全である。

【０３４９】なお、本実施形態では暗号鍵生成手段７０にパスワードも使用していたが、第１１の実施形態における変形例に対応させて、特徴データ６７だけで暗号鍵を生成するようにしてもよい。本実施形態では指紋を用いて暗号化された鍵について取り扱ったが、本発明は指紋に限られるものでなく、声紋や虹彩等、本人を特定できるものであれば、種々の生体データを利用して本人認証を行うようにしてもよい。

【０３５０】（第１３の実施の形態）本実施形態は、第１１及び第１２の実施形態のシステムにおける指紋読取り機６４で読み取った情報から指紋６５を生成する手段と、指紋６５から特徴抽出を行う特徴抽出手段６６とについて説明する。

【０３５１】図３１は本発明の第１３の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図であり、図４、図７、図９、図１１、図１３、図１５、図１６、図２７及び図２９と同一部分には同一符号を付し、その説明を省略する。また、本実施形態のシステムには、図２に示す文書認証システム１０１、図３に示す外部認証システム１０２あるいは図６に示す認証文書認証システム１０３が用いられている。本実施形態の独自な機能部分は、文書認証プログラム１３３、外部認証プログラム１３４あるいは認証文書確認プログラム１３５に修正が加えられたことによるものである。

【０３５２】この電子文書の改竄防止システムは、図１に示す文書認証システム１０１、外部認証システム１０２あるいは認証文書確認システム１０３と同様な構成に、以下に各手段が付加されて構成される。なお、以下、文書認証システム１０１の場合を例にとって説明する。

【０３５３】図３１に示す文書認証システム１０１は、指紋読取り機６４からの指紋原データ８７Ｆから指紋６５を生成する指紋データ抽出手段８７と、指紋６５から特徴データ６７を抽出する特徴抽出手段６６とによって構成されている。

【０３５４】指紋データ抽出手段８７には、境界抽出手段８７Ａと、エンボス手段８７Ｅと、輪郭抽出手段８７Ｌと、２値化手段８７Ｂとが設けられている。

【０３５５】一方、特徴抽出手段６６には、指紋６５からデータ６６ＳＤを切り出す領域切り出し手段６６Ｓと、切り出されたデータ６６ＳＤと予め用意されたパターン６６Ｐとをマッチングさせるマッチング手段６６Ｍと、マッチング手段６６Ｍにより生成された一桁分データ６６Ｄから特徴データ６７を生成する手段（図示せず）とが設けられている。

【０３５６】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図３１、図３２、図３３、図３４及び図３５を用いて説明する。

【０３５７】図３２は指紋データ６５の一例を示す図である。

【０３５８】図３３は指紋データ６５から矩形領域に切り出したデータ６６ＳＤの一例を示す図である。

【０３５９】図３４はマッチングさせるパターンの例の一部分を示した図である。

【０３６０】図３５は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【０３６１】図３５において、まず、指紋読み取り機６４により指紋についてのデータが読取られ、指紋原データ８７Ｆが得られる（Ｅ１）。

【０３６２】次に境界抽出手段８７Ａにより指紋データの境界が明確にされ（Ｅ２）、さらにエンボス手段８７

Ｅにより境界を明確にしたデータのエンボスが取られる（Ｅ３）。次にデータの輪郭抽出が行われ（Ｅ４）、さらに抽出データが２値化されて指紋データ６５を得る（Ｅ５）。図３２にこの様にして得た指紋データ６５のサンプルが示される。

【０３６３】次に、領域切り出し手段６６Ｓによって領域が指定されつつデータ６６ＳＤの切り出しが行われる（Ｅ６）。この様にして切り出したデータのサンプルが図３３に示される。

【０３６４】次にマッチング手段６６Ｍによりデータ６６ＳＤとパターンデータ６６Ｐとのパターンマッチングが行われる（図３５Ｅ７）。図３４にマッチングを行うパターンの一例が示される。パターンマッチチングが成立すると、マッチング手段６６Ｍからマッチングデータを取り出してこれを１桁データ６６Ｄとする（Ｅ８）。

【０３６５】次に、特徴データを生成するのに必要な桁数が指紋６５から読み出されたかが調べられ、まだデータが有る場合にはステップＥ６～Ｅ８が繰り返される（Ｅ９）。必要な桁数を読み終わると（Ｅ９）、１桁データ６６Ｄから生成される特徴データ６７が出力される。

【０３６６】以上により指紋データ６５から暗号鍵を生成する為の特徴データ６７の生成が行われる。

【０３６７】上述したように、本発明の実施の形態に係る電子文書の改竄防止システム及び方法は、指紋データ６５から暗号鍵を生成する為の特徴データ６７を生成することができるので、これを第１１及び第１２の実施形態における本人認証及び秘密鍵復号システムに利用でき、その効果は非常に大きい。

【０３６８】［第１４～第１７の実施形態についての説明］上記第１～第１３の実施形態に説明した発明によれば、文書作成した本人以外に外部認証機関の認証を追加することで、作成した本人による文書改竄をも防止することができ、重要書類を電子化することが可能となる。

【０３６９】しかし、作成した文書に別の作者が一部変更を加えて、新しい文書にする時には、元の作者と新しい作者及び外部認証機関が再び認証を行なう必要がある。

【０３７０】そこで、以下の第１４～１７の実施形態においては、改竄防止の為に認証を行なった電子文書及びデータの変更に関し、オリジナルの作者以外の変更者により電子文書が変更される場合に、当該オリジナル作者の認証を維持しつつ変更電子文書の再認証を可能とする方法及びシステムについて説明する。すなわち以下の実施形態では、複数の作者が複数の時期に渡って作成した電子文書の変更履歴を明らかにしつつ信用性を付与すると共に取り扱い性を高め、従来紙でしかできなかった履歴文書等の変更文書の電子化を実現する。

【０３７１】図３６は本発明の第１４～第１７の実施形態における文書変更を含んだ電子文書の改竄防止システム及び方法の全体的な構成を示す図である。

【０３７２】同図に示すように、公衆回線や専用回線を用いたネットワーク１１００が構成され、当該ネットワークに文書認証システム１１０１や外部認証機関１０９９の外部認証システム１１０２、文書変更認証システム１１０３、認証文書確認システム１１０４が接続されている。

【０３７３】文書認証システム１１０１は、第１～第１３の実施形態で説明した文書認証システム１０１と同様に構成されたシステムである。外部認証システム１１０２は文書認証システム１１０１から認証すべき情報を受信して、認証した結果を返信する。また、外部認証システム１１０２はネットワーク１１００を介して、文書変更認証システム１１０３から認証すべき情報を受信して、認証した結果を返信する。

【０３７４】文書認証システム１１０１、文書変更認証システム１１０３、認証文書確認システム１１０４は複数存在してよく、異なった使用者によって使用される。

【０３７５】また、文書認証システム１１０１、外部認証システム１１０２、文書変更認証システム１１０３、及び認証文書確認システム１１０４は、ワークステーションやパーソナルコンピュータなどの計算機に表示装置、入力装置、あるいは例えば指紋読取装置、スキャナ装置などを付加したものであり、基本的には動作プログラムが異なる事で異なる各機能を実現する。従って、文書認証システム１１０１、文書変更認証システム１１０３、認証文書確認システム１１０４は一つの計算機上に構成される場合も有る。

【０３７６】さらに、文書変更認証システム１１０３及び外部認証システム１１０２とを同一計算機、あるいはＬＡＮ等で接続される計算機上に構成させ、外部認証機関において、認証作業の全てを行うようにする事も可能である。

【０３７７】本発明に関わる電子文書の変更認証システム及び方法は、これらの文書認証システム１１０１、外部認証システム１１０２、文書変更認証システム１１０３及び認証文書確認システム１１０４を適宜組み合わせ、あるいはその一部機能を適宜組み合わせて成るものである。さらに本明細書では、便宜上、第１～第１３の実施形態と第１４～第１７の実施形態とにわけて説明しているが、両実施形態グループに属する各システムを適宜組み合わせ、あるいはその一部機能を適宜組み合わせ又組み込むことも可能である。

【０３７８】また、上記場合はネットワークを介した情報の瞬時転送を前提とした場合を説明しているが、図３６に示す様にフロッピーディスク等の記録媒体９７，９８を介して文書変更認証システム１１０１～外部認証システム１１０２間、あるいは文書認証システム１１０１～文書変更認証システム１１０３間、文書変更認証システム１１０３～認証文書確認システム１１０４間で必要

情報の交換を行う事も可能である。

【０３７９】全体的には以上のシステム構成を有する文書変更を含んだ電子文書の改竄防止システム及び方法について、対応する第１４～第１７の実施形態を説明する。

【０３８０】(第１４の実施の形態)本実施形態は改竄を防止できる電子文書の変更システム及び方法に関するものである。

【０３８１】図３７は本発明の第１４の実施形態に係る文書変更を含んだ電子文書の改竄防止システムに適用される文書変更認証システムのハードウェア構成例を示すブロック図である。

【０３８２】文書変更認証システム１１０３は、計算機１１１０に、表示装置１１１１、入力装置１１１２、印刷装置１１１３、外部記憶装置１１１４、指紋読み取り機１０６４、スキャナ１１１５が接続されてなっている。

【０３８３】この文書変更認証システム１１０３の上記ハードウェア構成は、図２に示す文書認証システム１０１と同様なものであり、ここでは説明を省略する。すなわち、計算機１１１０、表示装置１１１１、入力装置１１１２、印刷装置１１１３、外部記憶装置１１１４、指紋読み取り機１０６４、スキャナ１１１５が、それぞれ計算機１１０、表示装置１１１、入力装置１１２、印刷装置１１３、外部記憶装置１１４、指紋読み取り機６４、スキャナ１１５に対応する。

【０３８４】また、計算機１１１０内の構成についても同様であり、文書変更認証システム１１０３の各構成要素１１１６～１１３３が、文書認証システム１０１の各構成要素１１６～１３３に対応している。

【０３８５】ただし、ハードディスク装置１１２８やＲＡＭ１１１９等に格納されるソフトウエア的要素のうち、文書変更認証システム１１０３に対応する部分は本実施形態独自のものとなる。すなわちプログラム格納部１１３０は文書変更認証システム１１０１を実現するプログラム等を格納し、また、ＲＡＭ１１１９は、文書変更認証プログラム１１３３を格納する。なお、第１実施形態と同様に、この文書変更認証プログラム１１３３は、ハードディスク装置１１２８のプログラム格納部１１３０から呼び出され、ＲＡＭ１１１９内に格納される。

【０３８６】また、ＣＰＵ１１１７は、ＲＡＭ１１１９内の文書変更認証プログラム１１３３に従って各部を制御し、文書変更認証システム１１０３を実現する。

【０３８７】本実施形態及び以下の各実施形態における処理説明図や流れ図などに表現される各手段（各処理）あるいは図示しない各手段（各処理）は、主として文書変更認証プログラム１１３３に従うＣＰＵ１１１７の動作による機能実現手段である。

【０３８８】次に外部認証システムのハードウェア構成について説明する。

【０３８９】図３８は本実施形態の文書変更を含んだ電子文書の改竄防止システムに適用される外部認証システムのハードウェア構成例を示すブロック図であり、図３７と同一部分には同一符号を付してその説明を省略する。

【０３９０】外部認証システム１１０２は、文書変更認証システム１１０３と同様な計算機システムから構成される。文書変更認証システム１１０３との相違点は、ハードディスク装置１１２８のプログラム格納部に格納される動作プログラムである。この動作プログラムが呼び出され、ＲＡＭ１１１９内に外部認証プログラム１１３４として格納される。ＣＰＵ１１１７は、この外部認証プログラムに従って各部を制御し、外部認証システム１１０２が実現される。また、ソフトウェア資源（特に外部認証プログラム１１３４）とハードウェア資源とが結合して機能実現手段が構成される点も文書変更認証システム１１０３の場合と同様である。

【０３９１】次に図３９及び図４０を用いて文書変更を含んだ電子文書の改竄防止システムの各構成について説明する。

【０３９２】図３９及び図４０は本実施形態の文書変更を含んだ電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図である。

【０３９３】この文書変更を含んだ電子文書の改竄防止システムは文書変更認証システム１１０３と外部認証システム１１０２とから構成されている。

【０３９４】まず図３９の構成を説明する。

【０３９５】文書変更認証システム１１０３は、分離手段１００５と、変更者#nの変更及び認証手段１００６と、結合手段１００９とから構成され、変更履歴付電子文書１００１から変更履歴付電子文書１０１１を生成するようになっている。

【０３９６】ここで変更履歴付電子文書１００１は、過去に変更があった電子文書あるいは過去に変更はないがこれから変更を施す電子文書であって、認証付き原電子文書１００２と、1回目変更からn-1回目変更までの認証付き変更箇所データ１００３と、n-1回目の認証付き変更電子文書１００４とから構成されている。

【０３９７】分離手段１００５は、変更履歴付電子文書１００１を各構成要素に分離する。

【０３９８】変更者#nの変更及び認証手段１００６は、n-1回目の認証付き変更電子文書１００４を外部認証システム１０２に送出し、その応答結果に基づき、変更者#nによるn回目変更箇所１００７、変更者#n によるn回目変更電子文書１００８を出力する。

【０３９９】結合手段１００９は、認証付き原電子文書１００２と、1回目変更からn-1回目変更までの認証付き変更箇所データ１００３と、変更者#n によるn回目変更箇所１００７と、変更者#n によるn回目変更電子文書１

００８とを結合して変更履歴付電子文書１０１１を生成する。ここで、変更履歴付電子文書１０１１は、認証付き原電子文書１００２と、1回目からn回目までの変更箇所１０１０と、n回目変更電子文書１００８とから構成される。

【０４００】次に、図４０を用いて変更者#nの変更及び認証手段１００６の詳細構成及び外部認証システム１１０２の概略構成を説明する。

【０４０１】変更者#nの変更及び認証手段１００６は、文書変更手段１０２１と、差分抽出手段１０２３と、変更者認証手段１０２５Ａ，１０２５Ｂと、結合手段１０２８とを備えている。

【０４０２】文書変更手段１０２１は、変更電子文書１０２０を変更者#nによる変更電子文書１０２２に変換する。差分抽出手段１０２３は、変更電子文書１０２０と変更者#nによる変更電子文書１０２２との差分を抽出し、この差分データから構成されるn回目変更箇所１０２４を生成する。

【０４０３】変更者認証手段１０２５Ａ，１０２５Ｂは、それぞれ変更者の認証データで変更電子文書１０２２、変更箇所１０２４を認証し、変更者認証データ１０２６Ａ、変更者差分認証データ１０２６Ｂを出力する。

【０４０４】結合手段１０２８は、認証データ１０２７と変更者認証データ１０２６Ａとを結合し、結合認証データ１０２９を出力する。

【０４０５】特に図示しないが、変更者#nの変更及び認証手段１００６は、さらに、n-1回目の認証付き変更電子文書１００４から変更電子文書１０２０及び認証データ１０２７を取り出す手段と、変更箇所１０２４と認証データ１０３２Ｂを結合して変更箇所１００７を生成する手段と、変更電子文書１０２２と認証データ１０３２Ａとを結合して変更電子文書8を生成する手段とを備えている。

【０４０６】一方、外部認証システム１０２は、認証データ１０２９に対し、外部認証機関による認証を行って認証データ１０３１Ａを生成する外部認証手段１０３０Ａと、変更者差分認証データ１０２６Ｂに対し、外部認証機関による認証を行って認証データ１０３１Ｂを生成する外部認証手段１０３０Ｂとを備えている。

【０４０７】なお、認証データ１０２９及び変更者差分認証データ１０２６Ｂは、文書変更認証システム１１０３から外部認証システム１１０２に送信され、その認証結果１０３１Ａ，１０３１Ｂが外部認証システム１１０２から返信されるようになっている。

【０４０８】次に、図４１を用いて、変更者#nの変更及び認証手段１００６の変更者認証手段１０２５Ａについて説明する。

【０４０９】図４１は変更者#nの変更及び認証手段における変更者認証手段の構成を示す図である。

【０４１０】変更認証手段１０２５Ａは、変更者#nの秘密鍵１０２５Ａ－３及び見出し１０２６Ａ－Ｈを保持するとともに、特徴抽出手段１０２５Ａ－１及び暗号化手段１０２５Ａ－４を備えている。

【０４１１】特徴抽出手段１０２５Ａ－１は、変更電子文書２２から特徴データ１０２５Ａ－２を抽出して暗号化手段１０２５Ａ－４に引き渡す。暗号化手段１０２５Ａ－４は、特徴データ１０２５Ａ－２を変更者#nの秘密鍵１０２５Ａ－３で暗号化して暗号データ１０２６Ａ－Ｄを生成する。

【０４１２】変更認証手段１０２５Ａは、暗号データ１０２６Ａ－Ｄに見出し１０２６Ａ－Ｈを付加して、変更者の認証データ１０２６Ａを生成する。

【０４１３】なお、変更者認証手段１０２５Ｂについては特に図示しないが、変更者認証手段１０２５Ａと同様に構成される。

【０４１４】図４２は外部認証システムにおける外部認証手段の構成を示す図である。

【０４１５】外部認証手段１０３０Ａは、認証実行ＩＤを含む外部認証データ１０３０Ａ－Ａ及び外部認証機関の秘密鍵１０３０Ａ－２を保持するとともに、結合手段１０３０Ａ及び暗号化手段１０３０Ａ－３を備えている。

【０４１６】文書変更認証システム１１０３から送信される結合認証データ１０２９は、見出し１０２６Ａ－Ｈ及び暗号データ１０２６Ａ－Ｄからなる変更者の認証データ１０２６Ａと、認証データ１０２７とから構成されている。この結合認証データ１０２９は、外部認証手段１０３０Ａにて、見出し１０３１Ａ－Ｈと、暗号データ１０２６Ａ－Ｄ及び認証データ１０２７とに分離される。

【０４１７】暗号化手段１０３０Ａは、外部認証データ１０３０Ａ－Ａと、暗号データ１０２６Ａ－Ｄ及び認証データ１０２７とを結合し、暗号化手段１０３０Ａ－３は、この結合結果を秘密鍵１０３０Ａ－２で暗号化する。

【０４１８】外部認証手段１０３０Ａにより最終的に生成される外部認証機関の認証データ１０３１Ａは、見出し１０３１Ａ－Ｈと、暗号化手段１０３０Ａ－３により暗号化された暗号データ１０３１Ａ－Ｄからなる。

【０４１９】なお、外部認証手段１０３０Ｂについては特に図示及び説明しないが、これは外部認証手段１０３０Ａにおけるとを読み替えたものと同じである。

【０４２０】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図３９～図４３を用いて説明する。

【０４２１】図４３は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【０４２２】まず、文書変更認証システム１１０３において、変更履歴付電子文書１００１の読み込みが行われる（ＳＳ１）。

【０４２３】次に、分離手段１００５によって、変更履歴付原電子文書１００２、変更履歴付n-1回目までの変更箇所１００３及び変更履歴付n-1回目の変更電子文書１００４に分離される（ＳＳ２）。

【０４２４】次のステップＳＳ３からＳＳ７までの処理は変更及び認証手段１００６によって行われる。すなわち、図３９及び図４０に示すように、変更者#n(以下、複数存在し得る同種類の構成やデータには、場合により#1、#2、..あるいは第1の、第2の、..と記して区別する)が使用する変更及び認証手段6により、取り出されたn-1回目の認証付き変更電子文書１００４が変更され及び変更者#nの認証が行われ、変更者#nの認証データが外部認証システム１１０２に送信される。

【０４２５】具体的にはまず、n-1回目の認証付き変更電子文書１００４から、n-1回目変更電子文書１０２０が取り出される。さらに。変更者#nの入力操作で変更手段１０２１により、n-1回目の変更電子文書１０２０が変更され、n回目の変更電子文書１０２２が生成される（ＳＳ３）。

【０４２６】次に、差分抽出手段１０２３により、n-1回目の変更電子文書１０２０とn回目の変更電子文書１０２２と差分の抽出が行なわれ、n回目変更箇所１０２４の差分データが抽出される（ＳＳ４、図４０）。

【０４２７】この処理（ＳＳ４）は、次にようにしてなされる。すなわち各電子文書は詰まる所0と1から構成されるバイナリデータである。差分抽出手段１０２３は、これらバイナリデータの差分を抽出して、n回目変更箇所データ１０２４を出力する。これによりn回目変更箇所データ１０２４には、n-1回目変更電子文書１０２０とn回目変更電子文書１０２２の間でどの場所でどのデータが削除されたか、どの場所でどのデータが挿入されたか、どの場所でどのデータが入れ替えられたかの情報が保存される。

【０４２８】次に、変更者#nによる文書変更完了後の認証行われ、n回目変更電子文書１０２２とn回目変更箇所１０２４からそれぞれn回目変更電子文書の変更者認証データ１０２６Ａとn回目変更箇所の変更者認証データ１０２６Ｂが生成される（ＳＳ５、図４０）。

【０４２９】すなわちn回目変更電子文書１０２２が変更者認証手段１０２５Ａに与えられ、n回目変更者認証データ１０２６Ａが生成される。このためにまず、特徴抽出手段１０２５Ａ－１によってn回目変更変更電子文書１０２２の特徴データ１０２５Ａ－２が抽出される（図４１）。この特徴データ１０２５Ａ－２はn回目変更変更電子文書１０２２のどの1ビットが変化してもその値が異なった値となる様な電子文書自体の特徴を示すデータである。一方、見出し１０２６Ａ－Ｈは、特徴データ１０２５Ａ－２がn回目変更変更電子文書１０２２に属するデータである事をわかるようにする為に追加されるデータである。

【０４３０】次に、特徴データ１０２５Ａ－２は、変更者#nの秘密鍵１０２５Ａ－３を使用して暗号化手段１０２５Ａ－４で暗号化され、暗号データ１０２６Ａ－Ｄとして出力される。変更者#nの秘密鍵１０２５Ａ－３は、文字通り、変更者#n以外には知らせない様にした鍵で、変更者#nの公開鍵と対を成すものである。見出し１０２６Ａ－Ｈと暗号データ１０２６Ａ－Ｄとは対応しており、まとめて変更者認証データ１０２６Ａとして出力される。

【０４３１】同様にして、変更者認証手段１０２５Ｂによってn回目変更箇所データ１０２４から特徴が抽出され、 n回目変更者差分認証データ１０２６Ｂが生成される。

【０４３２】次に、n-1回目の認証付き変更電子文書１００４から取り出したn-1回目の変更電子文書認証データ１０２７と、n回目の変更電子文書の変更者認証データ１０２６Ａと結合手段２８によりが結合され、n回目の結合認証データ１０２９が生成される（ＳＳ６、図４０）。

【０４３３】次に、 n回目の結合認証データ１０２９とn回目変更箇所の変更者認証データ１０２６Ｂとが文書変更認証システム１１０３の通信装置１１２９を介してネットワーク１１００を通り外部認証システム１１０２に送信される（ＳＳ７）。

【０４３４】次のステップＳＳ８からＳＳ１０までの処理は外部認証システム１１０２において行われる。

【０４３５】まず、外部認証システム１１０２は文書変更認証システム１１０３から送られたn回目変更文書の変更者結合認証データ１０２９とn回目変更者差分認証データ１０２６Ｂを受信する（ＳＳ８）。

【０４３６】次に、外部認証システム１１０２において、送られたn回目の結合認証データ１０２９とn回目変更箇所の変更者認証データ１０２６Ｂとがそれぞれ外部認証手段１０３０Ａ、１０３０Ｂにより認証され、それぞれ認証データ１０３１Ａ、１０３１Ｂが生成される（ＳＳ９、図４０）。以下にこの処理を説明する。

【０４３７】このためにまず、外部認証手段１０３０Ａによって、n回目変更文書の変更者結合認証データ１０２９から見出し１０３１Ａ－Ｈが取り出される。引き続いて、残りの暗号データ/認証データ１０２６Ａ－Ｄ／１０２７が結合手段１０３０Ａ－１に与えられる（図４２）。

【０４３８】この暗号データ/認証データ１０２６Ａ－Ｄ／１０２７に、外部認証機関の外部認証データ１０３０Ａ－Ａ（認証実行ＩＤ）が結合手段１０３０Ａ－１により結合される。なお、この認証実行識別情報としての認証実行ＩＤは原則として認証毎に異なるものであり、どの認証に対してとの認証実行ＩＤを付与したかは、外部認証機関１０９９に保存される。

【０４３９】次に、この結合データが、外部認証機関の

秘密鍵１０３０Ａ－２を用いて暗号化手段１０３０Ａ－３により暗号化され、暗号データ１０３１Ａ－Ｄが生成される。

【０４４０】ここで、外部認証データ１０３０Ａ－Ａは文書変更認証システム１１０３が認証を要求してきたデータに対して第三者である外部認証機関が認証した事を示す情報であり、認証した日付データが含まれる。見出し１０３１Ａ－Ｈと暗号データ１０３１Ａ－Ｄは、データの関係付けが行われ、n回目変更電子文書認証データ１０３１Ａとして出力される。

【０４４１】同様に、変更者差分認証データ１０２６Ｂも外部認証手段１０３０Ｂによって外部認証が与えられ、n回目差分認証データ１０３１Ｂとして出力される。この場合の外部認証手段１０３０Ｂの処理については、図４２のAをBと読み替えて説明を行なう。

【０４４２】すなわち外部認証手段１０３０Ｂでは、n回目変更文書の変更者結合認証データ１０２９を受け取る代わりに、 n回目変更者差分認証データ１０２６Ｂからデータを受け取ると、見出し１０３１Ｂ－Ｈを取り出して、残りの暗号データ１０２６Ｂ－Ｄが結合手段１０３０Ｂ－１に与えられる。前記暗号データ１０２６Ｂ－Ｄに外部認証機関の外部認証データ１０３０Ｂ－Ａが結合手段１０３０Ｂ－１により結合され、外部認証機関の秘密鍵１０３０Ｂ－２を用いて暗号化手段１０３０Ｂ－３により暗号化され暗号データ１０３１Ｂ－Ｄを生成する。ここで、外部認証データ１０３０Ｂ－Ａは文書変更認証システム１１０３が認証を要求してきたデータに対して第三者である外部認証機関が認証した事を示す情報であり、認証した日付データが含まれる。見出し１０３１Ｂ－Ｈと暗号データ１０３１Ｂ－Ｄはn回目差分認証データ１０３１Ｂとしてデータの関係付けが行われる。

【０４４３】こうして生成されたn回目変更電子文書認証データ１０３１Ａ及びn回目差分認証データ１０３１Ｂは、外部認証システム１１０２の通信装置１１２９を介してネットワーク１１００を通り文書変更認証システム１１０３に送信される（ＳＳ１０）。

【０４４４】文書変更認証システム１１０３においては、外部認証システム１１０２から送られたデータを認証データ１０３２Ａ、１０３２Ｂとして受信し、この受信データを変更及び認証手段１００６に与える（ＳＳ１１）。

【０４４５】次に、変更及び認証手段１００６において、n回目変更電子文書認証データ１０３１Ａはn回目変更電子文書１０２２との関係付けが行われ、n回目の認証付き変更電子文書１００８が生成され出力される。同様に、n回目差分認証データ１０３１Ｂはn回目変更箇所データ１０２４との関係付けが行われ、n回目の認証付き差分認証データ１００７が生成され出力される（ＳＳ１２、図４０）。

【０４４６】次に、変更箇所データ１００７は、結合手段１００９によって、1回目変更からn-1回目変更までの認証付き変更箇所データ１００３と結合され、各々関係付けのなされた1回目からｎ回目までの認証付き変更箇所データ１０１０となる。さらに、結合手段１００９により、認証付き原電子文書１００２、1回目からｎ回目までの認証付き変更箇所データ１０１０およびｎ回目認証付き変更電子文書１００８が関係付けられたn回目変更履歴付電子文書１０１１が生成される（ＳＳ１３、図３９）。

【０４４７】なお、n+1の変更を実施する時には、変更履歴付電子文書１００１をn回目の変更履歴付き電子文書とすると、 n+1回目の変更履歴付き電子文書が変更履歴付電子文書１０１１として得られる。

【０４４８】上述したように、本発明の実施の形態に係る変更電子文書の改竄防止システム及び方法は、変更者により電子署名された変更文書を外部認証機関が認証する手順を踏んで追加的な認証を行うようにしたので、外部認証機関の認証日付にはまさしく変更者が変更文書を作成していた事が証明される。また、電子署名が無い場合であっても文書変更者本人の秘密鍵で特徴データの暗号化がなされ、これに対応する公開鍵で復号化される事になるので、何れにしても文書変更者の変更になる文書である事が認証される。

【０４４９】また、変更文書本体の改竄を行なうと改竄後の文書から抽出されるべき特徴データが変化し、先に認証用に抽出された特徴データ１０２５Ａ－２と異なるものになる事によって、変更文書本体の改竄の事実が検出できる。一方先に認証用に抽出された特徴データ１０２５Ａ－２は外部認証機関の認証データ１０３０Ａ－Ａとともに認証機関の秘密鍵１０３０Ａ－２で暗号化されているので、認証付き変更電子文書１００８に付されている認証データ１０３２Ａの改竄は不可能である。従って、たとえ本人であっても外部認証後には文書改竄が不可能になる。

【０４５０】これにより裁判の場で文書の正当性が証明できる、証拠能力のある変更電子文書が生成できるため、従来紙で保存していた重要文書や、証拠書類を電子化する事が可能となる。また、従来の紙の文書でも改竄の有無を判定するには高度な技術が必要とされたが、本発明になる電子文書の改竄防止システムでは電子的な手順を踏むだけで改竄の有無を確認できるので、改竄の有無を容易に証明できる。

【０４５１】さらに電子化により保管場所が削減できると共に、遠隔地への文書伝送が瞬時に行なえる様になり、コンピュータによる検索が行なえるようになる。こうして、商取引の信用向上、取り引きの迅速化を図る事ができる。

【０４５２】また、本実施形態の変更文書改竄防止システムでは、文書変更認証システム１１０３や外部認証システム１１０２に於いて伝送データの暗号化が行われる

ので、ネットワーク１１００として公衆回線を用いても安全である。

【０４５３】さらに、本実施形態の変更文書改竄防止システムでは、文書変更認証システム１１０３と外部認証システム１１０２との間でやり取りされるデータは文書データではなく、文書データの特徴（差分データ等）であるので、文書データそのものの内容はネットワーク１１００や外部認証システム１１０２に流す必要が無く、文書データの秘密を保つ事ができる。

【０４５４】さらに、外部認証機関が認証した外部認証データを元の変更電子文書と変更箇所に結合して認証付きの変更履歴付文書１０１１の形で管理するようにしたので、電子文書を保存する時の扱いが楽になる。

【０４５５】（第１５の実施の形態）本実施形態では、第１４の実施形態で認証した認証付き変更電子文書１０１１が真正なものである事を確認し、また外部認証機関の付した認証日付などの認証情報を取り出すシステムについて説明する。

【０４５６】この変更電子文書の改竄防止システムは、図３６に示した認証文書確認システム１１０４として構成されるものである。

【０４５７】図４４は本発明の第１５の実施の形態に係る変更電子文書の改竄防止システムに適用される認証文書確認システムのハードウェア構成例を示すブロック図であり、図３７と同一部分には同一符号を付してその説明を省略する。

【０４５８】認証文書確認システム１１０４は、文書変更認証システム１１０３と同様な計算機システムから構成される。文書変更認証システム１１０４との相違点は、ハードディスク装置１１２８のプログラム格納部１１３０に格納される動作プログラムである。この動作プログラムが呼び出され、ＲＡＭ１１１９内に認証文書確認プログラム１１３５として格納される。ＣＰＵ１１１７は、この認証文書確認プログラム１１３５に従って各部を制御し、認証文書確認システム１１０４が実現される。また、ソフトウェア資源とハードウェア資源とが結合して機能実現手段が構成される点も文書変更認証システム１１０３の場合と同様である。

【０４５９】次に図４５～図４７を用いて電子文書の改竄防止システムの機能構成について説明する。

【０４６０】図４５は本実施形態の変更電子文書の改竄防止システムに適用される認証文書確認システムの機能構成ならびに処理流れの一例を示す図であり、図３９と同一部分には同一符号を付して説明を省略する。

【０４６１】同図において、認証確認の対象となる変更電子文書１０１１Ｂは、原電子文書１００２Ｂと、変更電子文書１００８Ｂと、1回目からn回目までの変更箇所１００７Ｂ#1～１００７Ｂ#n-1及び１００７Ｂとからなり、これは第１４の実施形態における変更電子文書１０１１に対応している。

【０４６２】一方、認証文書確認システム１１０４には、n回目の認証確認手段１０４０と、n-1回目の認証確認手段１０４０#n-1と、日付確認手段１０４１，１０４１#n-1と、同一性判定手段１０４２，１０４２#n-1とが設けられる。さらに、認証文書確認システム１１０４には、繰返し部分となる認証確認手段１０４０と同様な認証確認手段１０４３と、第１～第１３の実施形態におけるものと同様な認証確認手段１０４４，日付確認手段１０４５及び同一性判定手段１０４６とが設けられている。

【０４６３】また、認証文書確認システム１１０４には、変更履歴付電子文書１０１１Ｂから認証付き原電子文書１００２Ｂと、1回目変更からn回目変更までの認証付き変更箇所データ１００７Ｂ#1，１００７Ｂ#2，…１００７Ｂ#n-1，１００７Ｂと、n回目の認証付き変更電子文書１００８Ｂとを取り出し、認証データと文書データと変更箇所データとに分解する手段(図示せず)が設けられている。

【０４６４】次に図４６及び図４７を用いて認証文書確認システム１１０４を構成する認証確認手段の各機能構成について説明する。

【０４６５】図４６は認証確認手段１０４０の詳細構成を示す図であり、図４７は認証確認手段１０４０#n-1の詳細構成を示す図である。

【０４６６】認証確認手段１０４０は、n回目の認証付き変更電子文書１００８Ｂの認証を確認する認証確認手段１０４０Ａと、n回目の認証付き変更箇所１００７Ｂの認証を確認する認証確認手段１０４０Ｂとから構成される。

【０４６７】認証確認手段１０４０Ａにおいては、認証データ１４０１Ａ、外部認証機関１０９９の公開鍵１４０２Ａ、見出しを含む変更者結合認証データ1404Ａ、変更者認証データ１４０６Ａ、以前の認証データ１４０７Ａ、変更者の公開鍵１４０８Ａ、特徴データ１４１０Ａ及び特徴データ１４１２Ａが保持されている。また、復号化手段１４０３Ａ、分離手段１４０５Ａ、復号化手段１４０９Ａ、特徴抽出手段１４１１Ａ及び照合手段１４１３Ａが設けられている。

【０４６８】ここで、見出しを含む変更者結合認証データ１４０４Ａは、見出し１４０１Ａ－Ｈと暗号データ１４０１Ａ－Ｄから構成される。また、見出しを含む変更者結合認証データ１４０４Ａは、見出し１４０４Ａ－Ｈと変更者結合認証データ１４０４Ａ－Ｄとから構成され、変更者結合認証データ１４０４Ａ－Ｄはさらに変更者結合認証データ１４０４Ａ－Ｄ１と外部認証機関１０９９の認証データ１４０４Ａ－Ｄ２とから構成される。以前の認証データ１４０７Ａは見出しと認証データ本体とから構成される。

【０４６９】一方、認証確認手段１０４０Ｂにおいては、認証データ１４０１Ｂ、外部認証機関１０９９の公

開鍵１４０２Ｂ、見出しを含む変更者認証データ１４０４Ｂ、変更者の公開鍵１４０８Ｂ、特徴データ１４１０Ｂ、特徴データ１４１２Ｂが保持されている。また、復号化手段１４０３Ｂ、復号化手段１４０９Ｂ、特徴抽出手段１４１１Ｂ、照合手段１４１３Ｂが設けられている。

【０４７０】ここで、見出しを含む変更者認証データ１４０１Ｂは見出し１４０１Ｂ－Ｈと暗号データ１４０１Ｂ－Ｄから構成される。見出しを含む変更者認証データ１４０４Ｂは見出し１４０４Ｂ－Ｈと変更者認証データ１４０４Ｂ－Ｄとから構成され、変更者認証データ１４０４Ｂ－Ｄはさらに変更者認証データ１４０４Ｂ－Ｄ１と外部認証機関１０９９の認証データ１４０４Ｂ－Ｄ２とから構成される。

【０４７１】次に図４７を用いて認証確認手段１０４０#n-1を説明する。

【０４７２】認証確認手段１０４０#n-1は、n-1回の認証データ１０２７の認証を確認する認証確認手段１０４０Ａと、n-1回目の認証付き変更箇所１００７Ｂ#n-1の認証を確認する認証確認手段１０４０Ｂとから構成される。

【０４７３】ここで、図４７における認証確認手段１０４０Ａ及び１０４０Ｂと図４６における認証確認手段１０４０Ａ及び１０４０Ｂとは同一の手段を使用するが、n-1回以前の認証データ１０２７の認証確認で使用しない機能は図示を省略している。

【０４７４】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について図４５～図５０を用いて説明する。

【０４７５】この認証文書確認システム１１０４においては、変更履歴付電子文書１０１１Ｂ内のn回目の認証付き変更電子文書１００８Ｂからスタートしてn回目の側から原文書の方向に向って順次認証の確認が繰返され、原文書と最終文書、および全ての変更箇所の電子文書の同一性確認が行われる。また、認証データから取り出された外部認証データから外部認証機関１０９９による認証の事実及びその認証日付１０４５，１０４１#1，１０４１#2，…１０４１#n-1，１０４１が確認される。

【０４７６】図４８は本実施形態の電子文書の改竄防止システムの動作を示す流れ図である。

【０４７７】同図においてまず、まず、外部記憶装置１１１４、ハードディスク装置１１２８から、あるいはネットワーク１１００を介して変更履歴付電子文書１０１１Ｂが読み込まれる（ＴＴ１）。この変更履歴付電子文書１０１１Ｂからは、認証付き原電子文書１００２Ｂと、1回目変更からn回目変更までの認証付き変更箇所データ１００７Ｂ#1，１００７Ｂ#2，…１００７Ｂ#n-1，１００７Ｂと、n回目の認証付き変更電子文書１００８Ｂとが取り出され、さらに認証データと文書データ、変更箇所データに分解される(ＴＴ２)。

【０４７８】次に、文書変更回数Ｎが最終の変更回数n回に設定され、認証確認初回フラグが設定される（ＴＴ３）。

【０４７９】ここで、初回の認証確認かどうかが判断される（ＴＴ５）。初回の場合にはＮ回目変更文書データ１００８Ｂの認証データ、Ｎ回目変更文書１００８Ｂの文書データ、Ｎ回目変更箇所１００７Ｂの変更認証データ、及びＮ回目変更箇所１００７Ｂの変更箇所データが認証確認手段１０４０に読み込まれる（ＴＴ６）。

【０４８０】続いて認証確認手段１０４０により認証確認が実行され、認証データ１０２７が出力され、少なくとも外部認証機関の日付と認証実行ＩＤを含んだ日付認証データ１０４１が生成される（ＴＴ８）。

【０４８１】一方、ステップＴＴ５で初回でない場合には、Ｎの数に応じてn-1回目変更箇所１００７Ｂ#N-1から1回目変更箇所１００７Ｂ#1までのどれかが認証確認手段１０４０に読み込まれる（ＴＴ７）。

【０４８２】続いて認証確認手段１０４０#n-1，１０４０#n-2…により認証確認が実行され、認証データ１０２７が出力され、日付認証データ１０４１#n-1，１０４１#n-2…が生成される（ＴＴ８）。ここで認証確認手段１０４１#n-1，１０４１#n-2…は同じ認証確認手段が繰り返し呼び出される。

【０４８３】ここで、n回目、n-1回目 及びn-2回目から1回目におけるステップＴＴ８の認定内容について簡単に説明する。

【０４８４】すなわちまず、n回目の認証付き変更電子文書１００８Ｂ及びn回目の認証付き変更箇所１００７Ｂの認証確認が認証確認手段１０４０により行われる。これにより、n-1回目までの認証データ１０２７が出力され、外部認証機関の認証日付１０４１が出力される。さらに、n回目変更電子文書１００８Ｂとn回目認証付き変更箇所１００７Ｂが、変更履歴付電子文書１０１１のn回目変更電子文書１００８とn回目認証付き変更箇所１００７と同一であるか否かの同一性判定１０４２が行われる。

【０４８５】また、 n-1回目の認証付き変更箇所１００７Ｂ#n-1の認証確認は、認証確認手段１００４#n-1により行われる。すなわち、n-2回目までの認証データ１０２７#n-1が出力され、外部認証機関の認証日付１０４１#n-1が出力される。さらに、n-1回目認証付き変更箇所１００７Ｂ#n-1が変更履歴付電子文書１０１１のn-1回目認証付き変更箇所１００７#n-1と同一であるか否かの同一性判定１０４２#n-1が行われる。

【０４８６】また、同様に認証確認手段１０４３により、n-2回目から1回目の認証付き変更箇所１００７Ｂ#1から１００７Ｂ#n-2に基づき、それぞれの回の認証データ及び外部認証機関の認証日付が出力される。さらに、認証付き変更箇所１００７Ｂ#1…１００７Ｂ#n-2が変更

履歴付電子文書１０１１の認証付き変更箇所１００７#1…１００７#n-2と同一であるか否かの同一性判定が行われる。

【０４８７】以上の何れかの認証確認（ＴＴ８）が実行された後、認証実行ＩＤの不一致または同一性判定手段１０４２の判定が否の場合（ＴＴ９）は、Ｎ回目文書の不一致が表示装置１１１１に表示されて終了する。なお、外部記憶装置１１１４に出力したり、ハードディスク装置１１２８に出力したり、ネットワーク１１００に出力したりして終了してもよい（ＴＴ１０）。

【０４８８】一方、認証実行ＩＤが一致しかつ同一性判定手段１０４２の判定が真の場合（ＴＴ９）には、認証確認初回フラグがクリアされ、変更回数Ｎを1減じる（ＴＴ１１）。

【０４８９】次に変更回数Ｎが１かどうかが判定され（ＴＴ１２）、Ｎが1より大きい場合にはステップＴＴ４に戻り、初回の認証確認かどうかが判断されて（ＴＴ５）、ステップＴＴ５～ステップＴＴ１２が繰り返される。

【０４９０】一方、変更回数Ｎが1の場合には（ＴＴ１２）、認証付き原電子文書１００２Ｂの認証データと文書データが認証確認手段１０４４に読み込まれる（ＴＴ１３）。なお、ここで与えられる認証データは認証確認手段１０４３から出力されるものであり、文書データは、認証付き原電子文書１００２Ｂから認証部分を除いたものである。

【０４９１】続いて、認証確認手段１０４４により認証確認が実行され、原文書の外部認証機関の日付認証データ１０４５が出力され、原電子文書１００２Ｂと原電子文書１００２とが同一であるか否かの同一性判定１０４６が行われる（ＴＴ１４）。なお、認証確認手段１０４４により認証確認処理は、先の実施形態におけるものと同様であるので説明を省略する。

【０４９２】ここで同一性判定手段１０４６の判定が否の場合（ＴＴ１５）には、原電子文書１００２Ｂが不一致である旨が表示装置１１１１に表示されて終了する。なお、外部記憶装置１１１４に出力したり、ハードディスク装置１１２８に出力したり、ネットワーク１１００に出力したりして終了してもよい（ＴＴ１６）。

【０４９３】一方、同一性判定手段１０４６の判定が真の場合（ＴＴ１５）には、文書一致である旨と、原電子文書の作成日付からn回目変更文書までの変更日付とが表示装置１１１１に表示されて終了する。また、外部記憶装置１１１４に出力したり、ハードディスク装置１１２８に出力したり、ネットワーク１１００に出力したりして終了してもよい（ＴＴ１７）。なお、認証日付は、認証確認手段１０４０Ａ，Ｂで得られた両者を表示してもよいし、片方を表示してもよい。また、両者の日付が一致している事を判定するようにしてもよい。

【０４９４】また、ステップＴＴ１７では原文書の作成者、各回の変更者の名前などを出力する様にしてもよい。

【０４９５】以上が本実施形態における認証文書確認システム１１０４の全体的な処理流れである。ここで次に図４８におけるステップＴＴ８の処理、つまり、認証確認手段１０４０及び１０４０#n-1の処理についてより具体的に説明する。

【０４９６】図４９は本実施形態の認証確認システムにおける認証確認手段１０４０Ａの処理を示す流れ図である。

【０４９７】同図は、認証確認手段１０４０及び１０４０#n-1の処理の双方を示しているが、ここでは認証確認手段１０４０の処理の場合を例にとって説明する。

【０４９８】まず、認証確認手段１０４０Ａにn回目の認証付き変更電子文書１００８Ｂから認証データの部分が入力される。この認証データ１４０１Ａは、n回目の認証付き変更電子文書１００８Ｂである事を分かる様にした見出し１４０１Ａ－Ｈと、暗号データ１４０１Ａ－Ｄとに分離される（Ｔ８０１、図４６）。なお、n-1…1回目変更の場合にあっては、後述するステップＴ８１１及びＴ８１２にて出力される以前の認証データ及び見出しが上記各データとして用いられる。

【０４９９】このうち、暗号データ１４０１Ａ－Ｄは外部認証機関１０９９の公開鍵１４０２Ａを用いた復号化手段１４０３Ａにより復号され、変更者結合認証データ１４０４Ａ－Ｄが出力される（Ｔ８０２、図４６）。このとき、変更者結合認証データ１４０４Ａ－Ｄと見出し１４０１Ａ－Ｈとは関係付けられ、認証データ１４０４Ａとなる（Ｔ８０３、図４６）。

【０５００】次に、変更者結合認証データ１４０４Ａ－Ｄにある外部認証データ１４０４Ａ－Ｄ２から少なくとも日付データと認証実行ＩＤが取り出され、日付認証手段１０４１に与えられる（Ｔ８０４、図４６）。

【０５０１】一方、変更者結合認証データ１４０４Ａ－Ｄの中の変更者認証データ１４０４Ａ－Ｄ１は分離手段１４０５Ａに与えられ、変更者認証データ１４０６Ａと以前の認証データ１４０７Ａ分離される（Ｔ８０５、図４６）。ここで、以前の認証データ１４０７Ａは原文書の認証からn-1回までの変更文書の認証を含むデータである。以前の認証データ１４０７Ａは認証確認手段１０４０#n-1に与える認証データ１０２７として出力される。

【０５０２】次に、認証確認初回フラグが確認され、初回の場合にはステップＴ８０７が実行され、初回でない場合には、ステップＴ８１０に移動する（Ｔ８０６）。

【０５０３】ステップＴ８０７が実行される場合には、復号化手段１４０９Ａにより、変更者認証データ１４０６Ａが変更者のn回目の公開鍵１４０８Ａで復号化されn回目の特徴データ１４１０Ａが生成される（Ｔ８０７、図４６）。

【０５０４】一方、最終回（ｎ回目）変更にあっては変更電子文書データ１００８Ｂから文書データの部分を受け取り、文書データの特徴が特徴抽出手段１４１１Ａにより抽出され、特徴データ１４１２Ａが出力される（Ｔ８０８、図４６）。なお、n-1 … 1回目変更にあっては認証データ１０２７，１０２７#n-1，…１０２７#2から特徴データが抽出される。

【０５０５】次に、復号化された特徴データ１４１０Ａと認証確認の為に特徴抽出された特徴データ１４１２Ａとが照合手段１４１３Ａにより照合され、その結果が同一性判定手段１０４２に出力される（Ｔ８０９）。同一性判定手段１０４２にて照合結果が一致と判定された場合には、変更電子文書１００８と変更電子文書１００８Ｂとが一致していると証明される。

【０５０６】さらに、認証確認手段１０４０Ａからは、以前の認証データ１４０７Ａが認証データ１０２７として出力され（Ｔ８１１）、今回の変更に関する見出し１４０４Ａ－Ｈが出力される（Ｔ８１２）。これらは、n-1 … 1回目変更の認証に用いられることになる。

【０５０７】次に認証確認手段１０４０のうち、認証確認手段１０４０Ｂ部分の処理を説明する。

【０５０８】図５０は本実施形態の認証確認システムにおける認証確認手段１０４０Ｂの処理を示す流れ図である。

【０５０９】同図は、認証確認手段１０４０及び１０４０#n-1の処理の双方を示しているが、ここでは認証確認手段１０４０の処理の場合を例にとって説明する。

【０５１０】まず、n回目の認証付き変更箇所１００７Ｂから認証データの部分が認証確認手段１０４０Ｂに入力される。この入力された認証データ１４０１Ｂは、n回目の認証付き変更箇所１００７Ｂである事を分かる様にした見出し１４０１Ｂ－Ｈと暗号データ１４０１Ｂ－Ｄとに分離される（Ｔ８２１、図４６）。

【０５１１】次に、暗号データ１４０１Ｂ－Ｄは、復号化手段１４０３Ｂに与えられ、外部認証機関１０９９の公開鍵１４０２Ｂが用いられて復号され、変更者認証データ１４０４Ｂ－Ｄが生成される（Ｔ８２２、図４６）。ここで公開鍵１４０２Ｂは公開鍵１４０２Ａと同じ内容のものである。

【０５１２】また、変更者認証データ１４０４Ｂ－Ｄと見出し１４０４Ｂ－Ｈとが関係付けられ、認証データ１４０４Ｂとされる（Ｔ８２３、図４６）。

【０５１３】変更者認証データ１４０４Ｂ－Ｄにある外部認証データ１４０４Ｂ－Ｄ２から少なくとも外部認証機関１０９９の日付データと認証実行ＩＤとが取り出され、日付認証手段１０４１に与えられる（Ｔ８２４、図４６）。

【０５１４】一方、変更者認証データ１４０４Ｂ－Ｄの中の変更者認証データ１４０４Ｂ－Ｄ１は、復号化手段１４０９Ｂに与えられる。復号化手段１４０９Ｂにおいては、n回目の変更者の公開鍵１４０８Ｂが使用されて、変更者認証データ１４０４Ｂ－Ｄ１が復号化されてn回目の変更箇所の特徴データ１４０１Ｂが取り出される（Ｔ８２７、図４６）。ここで公開鍵１４０８Ｂは公開鍵１４０８Ａと同じ内容のものである。

【０５１５】一方、最終回（ｎ回目）変更にあっては変更箇所データ１００７Ｂから変更箇所データの部分を受け取り、変更箇所データの特徴が特徴抽出手段１４１１Ｂにより抽出され、特徴データ１４１２Ｂが出力される（Ｔ８２８、図４６）。なお、n-1 … 1回目変更にあっては変更箇所データ１００７，１００７#n-1，…１００７#2から特徴データが抽出される。

【０５１６】次に、復号化された特徴データ１４１０Ｂと認証確認の為に特徴抽出された特徴データ１４１２Ｂとが照合手段１４１３Ｂにより照合され、その結果が同一性判定手段１０４２に出力される（Ｔ８２９）。同一性判定手段１０４２にて照合結果が一致と判定された場合には、変更箇所１００７と変更箇所１００７Ｂとが一致していると証明される。なお、より具体的には、認証確認手段１０４０Ａ，Ｂにおける両方の照合手段の結果が両方とも同一の判定である時にn-1回目からn回目の文書変更での文書改竄が無い事が証明されるものである。

【０５１７】さらに、認証確認手段１０４０Ｂからは、今回の変更に関する見出し１４０４Ｂ－Ｈが出力される（Ｔ８３２）。

【０５１８】以上は、主に認証確認手段１０４０による認証確認処理（図４８：ステップＴ８）を説明した。しかし、認証確認手段１０４０#n-1及び１０４３による認証確認処理ではこれと多少異なる部分があるので、その部分について図４７、図４８及び図４９を用いて説明する。

【０５１９】まずは、認証確認手段１０４０#n-1による処理について説明する。

【０５２０】認証確認手段１０４０から出力されたn-1回の認証データ１０２７が、図４７における認証データ１４０１Ａとして認証確認手段１０４０#n-1の認証確認手段１０４０Ａに与えられる。同一性判定手段１０４２#n-1に与えられる比較照合結果がただ一つである点を除けば、以下の処理は、認証確認手段１０４０の場合と同様である。なお、図４７における認証データ１４０７Ａは、認証データ１０２７として次の認証確認手段１０４３に与えられる。

【０５２１】また、認証確認手段１０４３では、認証確認手段１０４０#n-1と同様な処理が繰り返され、n-2回目から1回目までの認証確認が行われる。

【０５２２】上述したように、本発明の実施の形態に係る変更電子文書の改竄防止システム及び方法は、原文及び変更#1から変更#nまでの暗号化特徴データの付加と、原文作成者及び変更者#1から#nまでの本人認証及び外部認証機関の認証とがなされた変更電子文書から、nから1

に向かって順次外部認証機関の認証データを取り出し、また付加されている文書データの特徴データ及び変更箇所の特徴データと確認対象の電子文書本体からの特徴データ及び変更箇所の特徴データとを文書変更者#nから#1までの公開鍵を用いて照合するようにしたので、変更毎の外部認証機関の認証日付には、まさしく変更者#1から#nが文書変更を行なっていた事を証明することができる。

【０５２３】なお、電子文書本体の改竄を行なうと、電子文書１００８Ｂから抽出される特徴データ１４１１Ａが変化する事により、一方、特徴データ１４１０Ａは外部認証機関１０９９によって改竄を防止される事によって、変更者本人であっても外部認証後には文書改竄が不可能になる。

【０５２４】また、変更者#nが電子文書１００８Ｂの差し替えを行うと、外部認証機関１０９９が外部認証手段１０３０Ａ及び外部認証手段１０３０Ｂにより付加した認証実行ＩＤデータが変更若しくは消失していることが日付認証１０４１で発見される。したがって、当該差し替えは不可能である。また、原文１００２Ｂの認証は認証データ１０２７#1を使用するので、原文１００２Ｂ自体の改竄、差し替えも不可能である。

【０５２５】このように変更履歴付電子文書１０１１Ｂは変更者自身のみならず、外部認証機関、その他何人足りとも改竄をする事はできない。

【０５２６】これにより裁判の場で変更文書の原文から変更履歴全ての段階に於いて文書の正当性が証明でき、製造記録や検査記録等の同じ利害関係を持った複数人の変更記録に対しても証拠書類の電子化が可能となる。

【０５２７】また、外部認証機関の認証は特徴データに対して行なわれるので、外部に対して秘密を保持する事が必要な文書に対してもネットワーク１１００として公衆回線を使用しても安全である。

【０５２８】さらに、外部認証機関が認証した原文書、変更箇所、最終文書を結合する事により文書を保存する時の扱いが楽になる。

【０５２９】また、変更文書の各回の変更の認証確認が最終文書から順次遡って復元を行なう必要が無いので、認証の確認が高速で行なえる。

【０５３０】（第１６の実施の形態）本実施形態では、第１４の実施形態の変形例である変更文書の認証システムについて説明する。より正確には、図３９における変更者#nの変更及び認証手段１００６に関する変形例である。

【０５３１】図５１は本発明の第１６の実施形態の文書変更を含んだ電子文書の改竄防止システムにおける変更及び認証手段の機能構成及び処理流れを示す図であり、図４０と同一部分には同一の符号を付して説明を省略する。

【０５３２】図５１に示す文書変更を含んだ電子文書の改竄防止システムは、変更者#nの変更及び認証手段１００６において、図４０の変更者認証手段１０２５Ａに代えて特徴抽出手段１０３３及び変更者認証手段１０３４が設けられる他、第１４の実施形態と同様に構成されている。

【０５３３】ここで、特徴抽出手段１０３３は、変更文書１０２２の特徴を抽出する手段である。また、変更者認証手段１０３４は、結合手段１０２８から出力される結合データを変更者の暗号鍵で暗号化して認証し、認証データ１０２９を出力する手段である。なお、変更者認証手段１０３４は、図４０の変更者認証手段１０２５Ａと類似するものであって、特徴データ１０２５Ａ－２の代わりに、結合手段１０２８により出力される結合データを特徴抽出することなく暗号化するものである。

【０５３４】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について説明する。

【０５３５】まず、変更及び認証手段１００６に与えられたn-1回目の認証付き変更電子文書１００４から、n回目変更変更電子文書１０２２及び認証データ１０２７が得られるところまでは第１４の実施形態と同様である。

【０５３６】次に、n回目変更電子文書１０２２は特徴抽出手段１０３３に入力される。この特徴抽出手段１０３３により生成された特徴データは結合手段１０２８によって、認証データ１０２７と結合される。この結合手段１０２８によって結合されたデータは、変更者認証手段１０３４に与えられ暗号化されて、n回目変更文書の変更者結合認証データ１０２９が作成される。

【０５３７】以下、第１４の実施形態と同様な処理が行われる。

【０５３８】上述したように、本発明の実施の形態に係る変更電子文書の改竄防止システム及び方法は、第１４の実施形態と同様な構成を有する他、特徴抽出手段１０３３及び変更者認証手段１０３４を設けたので、第１４の実施形態と同様な効果が得られる他、変更文書本体の改竄を行なうと改竄後の文書から抽出されるべき特徴データが変化し、先に認証用に抽出された特徴データ１０３３と異なるものになる事によって、変更文書本体の改竄の事実を検出することができる。

【０５３９】また、一方先に認証用に抽出された特徴データ１０３３は外部認証機関の認証データ１０３０Ａ－Ａとともに認証機関の秘密鍵１０３０Ａ－２で暗号化されているので、認証付き変更電子文書１００８に付されている認証データ１０３２Ａの改竄は不可能である。従って、たとえ本人であっても外部認証後には文書改竄が不可能になる。

【０５４０】(第１７の実施の形態)本実施形態では、第１５の実施形態の変形例である変更文書の認証確認システムについて説明する。より正確には、図４５の認証確認手段１０４０及び１０４０#n-1に関する変形例であ

る。

【０５４１】図５２は本発明の第１７の実施形態の文書変更を含んだ電子文書の改竄防止システムにおける認証確認手段の機能構成及び処理流れを示す図であり、図４５と同一部分には同一の符号を付して説明を省略する。

【０５４２】図５２に示す文書変更を含んだ電子文書の改竄防止システムは、認証確認手段１０４０、１０４０#n-1及び１０４３において、分離手段１４０５Ａに代えて分離手段１４１４Ａが設けられる他、第１５の実施形態と同様に構成されている。

【０５４３】次に、以上のように構成された本発明の実施の形態に係る電子文書の改竄防止システムの動作について説明する。

【０５４４】まず、認証確認手段１０４０Ａにおいて、変更結合認証データ１４０４Ａが得られるところまでは、第１５の実施形態と同様である。

【０５４５】ここで、変更者結合認証データ１４０４Ａ－Ｄは、復号化手段１４０９Ａに与えられ、n回目の変更者の公開鍵１４０８Ａにより変更者結合認証データ復号される。復号データはさらに分離手段１４１４Ａによって分離され、特徴データ１４１０Ａと認証データ１４０７Ａとなる。

【０５４６】以下、第１５と同様な処理が行われる。

【０５４７】なお、認証確認手段１０４０#n-1及び１０４３においても、同様な処理が行われる。

【０５４８】上述したように、本発明の実施の形態に係る変更電子文書の改竄防止システム及び方法は、第１５の実施形態と同様な構成を有する他、分離手段１４０５Ａに代えて分離手段１４１４Ａを設けたので、第１５の実施形態と同様な効果を得ることができる。

【０５４９】なお、本発明は、上記各実施の形態に限定されるものでなく、その要旨を逸脱しない範囲で種々に変形することが可能である。

【０５５０】例えば各実施形態では単に電子文書１とのみ表現するが、この電子文書なるものは電子情報ならば文書に限らず何でもよい。例えば映像データ、音声データ、プログラムソースファイル、プログラム実行ファイル等のバイナリデータをも含む。

【０５５１】さらに、実施形態では主として公開鍵暗号方式の場合を説明しているが、本発明はこれに限られるものではなく、例えば秘密鍵暗号方式を用いてもよい。

【０５５２】また、実施形態に記載した手法は、計算機（コンピュータ）に実行させることができるプログラム（ソフトウエア手段）として、例えば磁気ディスク（フロッピーディスク、ハードディスク等）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤ等）、半導体メモリ等の記憶媒体に格納し、また通信媒体により伝送して頒布することもできる。なお、媒体側に格納されるプログラムには、計算機に実行させるソフトウエア手段（実行プログラムのみならずテーブルやデータ構造も含む）を計算機内に構成させる設定プログラムをも含むものである。本装置を実現する計算機は、記憶媒体に記録されたプログラムを読み込み、また場合により設定プログラムによりソフトウエア手段を構築し、このソフトウエア手段によって動作が制御されることにより上述した処理を実行する。

【０５５３】

【発明の効果】以上詳記したように本発明によれば、作成者本人自身による改竄をも防止した電子文書が提供できるので、重要文書や公的文書など従来は紙でなければ運用出来なかったものに対しても電子文書での運用が可能になり真の意味での電子化を実現させることを可能とした電子文書の改竄防止システム及び方法を提供することができる。

【０５５４】このように改竄を防止した電子文書化により、遠隔地でも重要文書を瞬時のうちに送達する事ができるようになる。また、電子契約書の実現により、契約書にサインを行う場合でも離れた場所で瞬時のうちにサインを交わす事ができる。電子文書化により文書の保管場所を取らなくなる。電子文書化により文書の検索が可能になる等、その効果は極めて大である。

【０５５５】また、本発明によれば、電子文書の特徴データからは電子文書の内容を伺い知る事ができないので、企業の秘密文書について外部認証機関の認証を行う事ができ、機密漏洩の危険から免れる事ができる電子文書の改竄防止システム及び方法を提供することができる。

【０５５６】さらに、本発明によれば、電子文書の特徴データを高速で作成でき、また圧縮率も高いので、特徴データ抽出時間とデータの伝送時間の短縮ができる電子文書の改竄防止システム及び方法を提供することができる。

【０５５７】さらにまた、本発明によれば、指紋データを使用し暗号鍵および秘密鍵を暗号化する事により本人認証データを盗まれる事が有っても他人にはそのデータを利用できないので、本人認証データの信頼性を非常に高くすることができる電子文書の改竄防止システム及び方法を提供することができる。

【０５５８】また、本発明によれば、複数人が複数時期に渡って一つの電子文書を作成する場合でも、変更文書を関係者全員で再承認する必要をなくしかつ文書改竄を防止して、紙文書の証拠能力以上の証拠能力を有する電子文書を作成可能とした電子文書の改竄防止システム及び方法を提供することができる。

【０５５９】このように作製者自身による改竄をも防止した変更電子文書が提供できるので、重要文書や公的文書など従来は紙でなければ運用できなかったものに対しても電子文書上での部分変更の運用が可能となる。また、各種設計資料や、設計図面、製作資料や製作図、試験資料や試験データ、試験結果、検査資料や検査結果など、企業の中で使用される文書で社外に開示をしたくな

い資料について、それらのドキュメントの内容と製作時期、変更内容と変更時期が証明されるので、製品事故などが発生した時の非常に有力な裁判資料として使用できる。とくに、設計工程、製造工程、検査工程の中等で、１枚の紙に複数の時期にわたって内容が追記されていくチェックシート等が裁判の場で正当性を証明できる資料としての電子化を実現する。

【図面の簡単な説明】

【図１】本発明の各実施形態における電子文書の作成システム及び方法の全体的な構成を示す図。

【図２】本発明の第１の実施の形態に係る電子文書の改竄防止システムに適用される文書認証システムのハードウエア構成例を示すブロック図。

【図３】同実施形態の電子文書の改竄防止システムに適用される外部認証システムのハードウエア構成例を示すブロック図。

【図４】同実施形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図５】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。

【図６】本発明の第２の実施の形態に係る電子文書の改竄防止システムに適用される認証文書確認システムのハードウエア構成例を示すブロック図。

【図７】同実施形態の電子文書の改竄防止システムに適用される認証文書確認システムの機能構成及び処理流れの一例を示す図。

【図８】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。

【図９】本発明の第３の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図１０】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。

【図１１】本発明の第４の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図１２】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。

【図１３】本発明の第５の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図１４】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。

【図１５】本発明の第６の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図１６】本発明の第７の実施形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図１７】同実施形態の電子文書の改竄防止システムの電子印鑑生成処理を示す流れ図。

【図１８】同実施形態の電子文書の改竄防止システムの電子印鑑照合処理を示す流れ図。

【図１９】同実施形態の電子文書の改竄防止システムの文書見出し編集処理を示す流れ図。

【図２０】本発明の第８の実施の形態の電子文書の改竄防止システムにおける特徴抽出方法を説明するための図。

【図２１】同実施形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図２２】同実施形態の電子文書の改竄防止システムの特徴データ抽出の処理の一例を示す流れ図。

【図２３】本発明の第９の実施の形態の電子文書の改竄防止システムにおける特徴抽出方法を説明するための図。

【図２４】本発明の第１０の実施の形態の電子文書の改竄防止システムにおける特徴抽出方法を説明するための図。

【図２５】同実施形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図２６】同実施形態の電子文書の改竄防止システムの特徴データ抽出の処理の一例を示す流れ図。

【図２７】本発明の第１１の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図２８】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。

【図２９】本発明の第１２の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図３０】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。

【図３１】本発明の第１３の実施の形態の電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図３２】指紋データの一例を示す図。

【図３３】指紋データから矩形領域に切り出したデータの一例を示す図。

【図３４】マッチングさせるパターンの例の一部分を示した図。

【図３５】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。

【図３６】本発明の第１４～第１７の実施形態における文書変更を含んだ電子文書の改竄防止システム及び方法の全体的な構成を示す図。

【図３７】本発明の第１４の実施形態に係る文書変更を含んだ電子文書の改竄防止システムに適用される文書変更認証システムのハードウェア構成例を示すブロック図。

【図３８】同実施形態の文書変更を含んだ電子文書の改竄防止システムに適用される外部認証システムのハードウェア構成例を示すブロック図。

【図３９】同実施形態の文書変更を含んだ電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。

【図４０】同実施形態の文書変更を含んだ電子文書の改竄防止システムの機能構成及び処理流れの一例を示す図。
【図４１】変更者#nの変更及び認証手段における変更者認証手段の構成を示す図。
【図４２】外部認証システムにおける外部認証手段の構成を示す図。
【図４３】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。
【図４４】本発明の第１５の実施の形態に係る変更電子文書の改竄防止システムに適用される認証文書確認システムのハードウェア構成例を示すブロック図。
【図４５】同実施形態の変更電子文書の改竄防止システムに適用される認証文書確認システムの機能構成ならびに処理流れの一例を示す図。
【図４６】認証確認手段１０４０の詳細構成を示す図。
【図４７】認証確認手段１０４０#n-1の詳細構成を示す図。
【図４８】同実施形態の電子文書の改竄防止システムの動作を示す流れ図。
【図４９】同実施形態の認証確認システムにおける認証確認手段１０４０Ａの処理を示す流れ図。
【図５０】同実施形態の認証確認システムにおける認証確認手段１０４０Ｂの処理を示す流れ図。
【図５１】本発明の第１６の実施形態の文書変更を含んだ電子文書の改竄防止システムにおける変更及び認証手段の機能構成及び処理流れを示す図。
【図５２】本発明の第１７の実施形態の文書変更を含んだ電子文書の改竄防止システムにおける認証確認手段の機能構成及び処理流れを示す図。
【図５３】電子文書に署名してその同一性を判定する従来の方法を示す図。
【符号の説明】
１…電子文書
２…特徴抽出手段
２Ｔ…セパレータテーブル
２Ｗ…単語配列
３…見出し付き特徴データ
３Ｈ…見出し
３Ｄ…特徴データ
４…秘密鍵
５…暗号化手段
６…見出し付き暗号データ
６Ｈ…見出し
６Ｄ…暗号データ
７…見出し付き認証データ
７Ｈ…見出し
７Ｄ…暗号データ
７Ａ…外部認証データ
８…秘密鍵
９…暗号化手段
１０…合成データ
１０Ｈ…見出し
１０Ｄ…暗号データ
１１…合成データ
１１Ｈ…見出し
１１Ｄ…暗号データ
１２…認証付電子文書
１３…公開鍵
１４…復号化手段
１５…見出し付き認証データ
１５Ｈ…見出し
１５Ｄ…暗号データ
１５Ａ…外部認証データ
１５Ａ－Ｄ…日付認証
１６…公開鍵
１７…復号化手段
１８…見出し付き特徴データ
１８Ｈ…見出し
１８Ｄ…特徴データ
１９…電子文書
２０…特徴抽出手段
２１…特徴データ
２２…照合手段
２２－Ｊ…同一性判定
２３…見出し付き認証データ
２３Ｈ…見出し
２３Ｄ…暗号データ
２３Ａ…外部認証データ
２４…秘密鍵
２５…暗号化手段
２６…見出し付き暗号データ
２６Ｈ…見出し
２６Ｄ…暗号データ
２７…見出し付き暗号データ
２７Ｈ…見出し
２７Ｄ…暗号データ
２８…認証付電子文書
２９…公開鍵
３０…復号化手段
３１…見出し付き認証データ
３１Ｈ…見出し
３１Ｄ…暗号データ
３１Ａ…外部認証データ
３１Ａ－Ｄ…日付認証
３２…見出し付き認証データ
３２Ｈ…見出し
３２Ｄ…暗号データ
３２Ａ…外部認証データ
３３…秘密鍵

３４…暗号化手段
３５…見出し付き暗号データ
３５Ｈ…見出し
３５Ｄ…暗号データ
３６…見出し付き認証データ
３６Ｈ…見出し
３６Ｄ…暗号データ
３６Ａ…外部認証データ
３７…秘密鍵
３８…暗号化手段
３９…見出し付き暗号データ
３９Ｈ…見出し
３９Ｄ…暗号データ
４０…見出し付き暗号データ
４０Ｈ…見出し
４０Ｄ…暗号データ
４１…認証付電子文書
４２…公開鍵
４３…復号化手段
４４…見出し付き認証データ
４４Ｈ…見出し
４４Ｄ…暗号データ
４４Ａ…外部認証データ
４４Ａ－Ｄ…日付認証
４５…公開鍵
４６…復号化手段
４７…見出し付き認証データ
４７Ｈ…見出し
４７Ｄ…暗号データ
４７Ａ…外部認証データ
４７Ａ－Ｄ…日付認証
４８…公開鍵
４９…復号化手段
５０…見出し付き特徴データ
５０Ｈ…見出し
５０Ｄ…特徴データ
５１…特徴抽出手段
５２…特徴データ
５３…照合手段
５３－Ｊ…同一性判定
５４…印影
５５…特徴抽出手段
５６…特徴データ
５８…暗号化手段
５９…暗号化印影
６０…電子印鑑
６１…日付署名印影情報
６２…整形手段
６３…文書表示手段
６４…指紋読取り機

６５…指紋
６６…特徴抽出手段
６６Ｓ…切り出し手段
６６ＳＤ…データ
６６Ｍ…マッチング手段
６６Ｐ…パターン
６６Ｄ…１桁分データ
６７…特徴データ
６８…パスワード
６９…氏名・ＩＤ
７０…暗号鍵生成手段
７１…暗号鍵
７２…乱数発生器
７３…秘密鍵公開鍵生成手段
７４…秘密鍵
７５…公開鍵
７６…暗号化手段
７７…暗号化秘密鍵
７８…本人認証データ
７８Ｆ…指紋
７８Ｓ…暗号化秘密鍵
７８Ｋ…暗号化暗号鍵
７８Ｐ…パスワード
７８Ｎ…氏名・ＩＤ
７９…表示手段
８０…照合手段
８１…照合手段
８２…判定ロジック
８３…復号手段
８４…暗号鍵
８５…照合手段
８６…復号手段
８７…指紋データ抽出手段
８７Ｆ…原指紋データ
８７Ａ…境界抽出手段
８７Ｅ…エンボス手段
８７Ｌ…輪郭抽出手段
８７Ｂ…２値化
９７，９８…記録媒体
９９…外部認証機関
１００…ネットワーク
１０１…文書認証システム
１０２…外部認証システム
１０３…認証文書確認システム
１１０…計算機
１１１…表示装置
１１２…入力装置
１１３…印刷装置
１１４…外部記憶装置
１１５…スキャナ

１１６…ＣＰＵバス
１１７…ＣＰＵ
１１８…ＲＯＭ
１１９…ＲＡＭ
１２０，１２１，１２２，１２３，１２４，１２５，１２６，１２７…インターフェース手段
１２８…ハードディスク装置
１２９…通信装置
１３０…プログラム格納部
１３１…データ格納部
１３２…作業領域
１３３…文書認証プログラム
１３４…外部認証プログラム
１３５…認証文書確認プログラム
１００１…変更履歴付電子文書
１００２…原電子文書
１００２Ｂ…認証確認対象の原電子文書
１００３…変更箇所
１００４…変更電子文書
１００５…分離手段
１００６…変更及び認証手段
１００７…変更箇所
１００７Ｂ…n回変更箇所
１００７Ｂ#n-1…n-1回変更箇所
１００８…変更電子文書
１００８Ｂ…認証確認対象の変更電子文書
１００９…結合手段
１０１０…変更箇所
１０１１…変更履歴付電子文書
１０１１Ｂ…認証確認対象の変更履歴付電子文書
１０２０…変更電子文書
１０２１…変更手段
１０２２…変更電子文書
１０２３…差分抽出手段
１０２４…変更箇所
１０２５Ａ，１０２５Ｂ…変更者認証手段
１０２５Ａ－１…特徴抽出手段
１０２５Ａ－２…特徴データ
１０２５Ａ－３…変更者#n秘密鍵
１０２５Ａ－４…暗号化手段
１０２６Ａ，１０２６Ｂ…変更者認証データ
１０２６Ａ－Ｈ…見出し
１０２６Ａ－Ｄ…暗号データ
１０２７…認証データ
１０２７#n-1…認証データ
１０２８…結合手段
１０２９…結合認証データ
１０３０Ａ，１０３０Ｂ…外部認証手段
１０３０Ａ－Ａ…外部認証データ
１０３０Ａ－１…結合手段

１０３０Ａ－２…外部秘密鍵
１０３０Ａ－３…暗号化手段
１０３１Ａ，１０３１Ｂ…認証データ
１０３１Ａ－Ｄ…暗号データ
１０３１Ａ－Ｈ…見出し
１０３２Ａ，１０３２Ｂ…認証データ
１０３３…特徴抽出手段
１０３４…変更者認証手段
１０４０…認証確認手段
１０４０Ａ，１０４０Ｂ…認証確認手段
１０４０#n-1…認証確認手段
１０４１…日付認証
１０４１#n-1…日付認証
１０４２…同一性判定
１０４２#n-1…同一性判定
１０４３…認証確認(繰返し)
１０４４…認証確認手段
１０４５…日付認証
１０４６…同一性判定
１０９７，１０９８…記録媒体
１０９９…外部認証機関
１１００…ネットワーク
１１０１…文書認証システム
１１０２…外部認証システム
１１０３…文書変更認証システム
１１０４…認証文書確認システム
１１１０…計算機
１１１１…表示装置
１１１２…入力装置
１１１３…印刷装置
１１１４…外部記憶装置
１１１５…スキャナ
１１１６…ＣＰＵバス
１１１７…ＣＰＵ
１１１８…ＲＯＭ
１１１９…ＲＡＭ
１１２０～１１２７…インターフェイス手段
１１２８…ハードディスク装置
１１２９…通信装置
１１３０…プログラム格納部
１１３１…データ格納部
１１３２…作業領域
１１３３…文書変更認証プログラム
１１３４…外部認証プログラム
１１３５…認証文書確認プログラム
１４０１Ａ…認証データ
１４０１Ａ－Ｄ…暗号データ
１４０１Ａ－Ｈ…見出し
１４０２Ａ…外部認証機関の公開鍵
１４０３Ａ…復号化手段

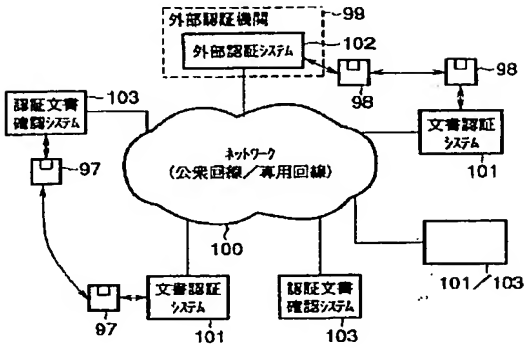
85

１４０４Ａ…変更者結合認証データ
１４０４Ａ－Ｄ…変更者結合認証データ
１４０４Ａ－Ｄ１…変更者認証データ
１４０４Ａ－Ｄ２…外部認証データ
１４０４Ａ－Ｈ…見出し
１４０５Ａ…分離手段
１４０６Ａ…変更者認証データ
１４０７Ａ…以前の認証データ
１４０８Ａ…変更者の公開鍵
１４１０Ａ…特徴データ
１４１１Ａ…特徴抽出手段
１４１２Ａ…特徴データ

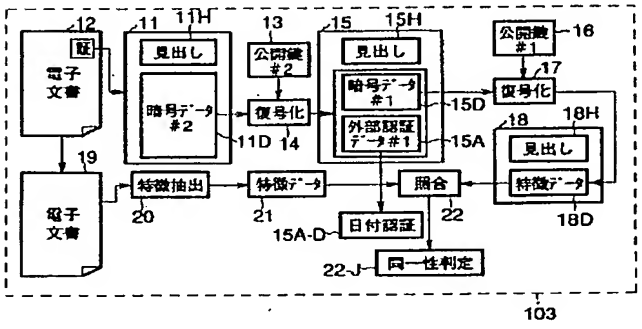
86

＊１４１３Ａ，１４１３Ｂ…照合手段
１４１４Ａ…分離手段
Ｓ…電子文書データ並び
Ｓ１，Ｓ２，Ｓ３…電子文書データ並び部分
Ｓ＿ｓｕｍ…合計値
Ｓ＿ｓ＿ｓｔｒｅａｍ…合計データ並び
ＩＳ…間隔を置いたデータ並び
ＩＳ１，ＩＳ２，ＩＳ３…間隔を置いたデータ並び部分
ＩＳ＿ｓｕｍ［０］，．．．，ＩＳ＿ｓｕｍ［２５５］…
間隔を置いたデータの合計値の配列
ＩＳ＿ｓ＿ｓｔｒｅａｍ…間隔を置いた合計データ並び
＊　ｉ，ｊ…カウンタ

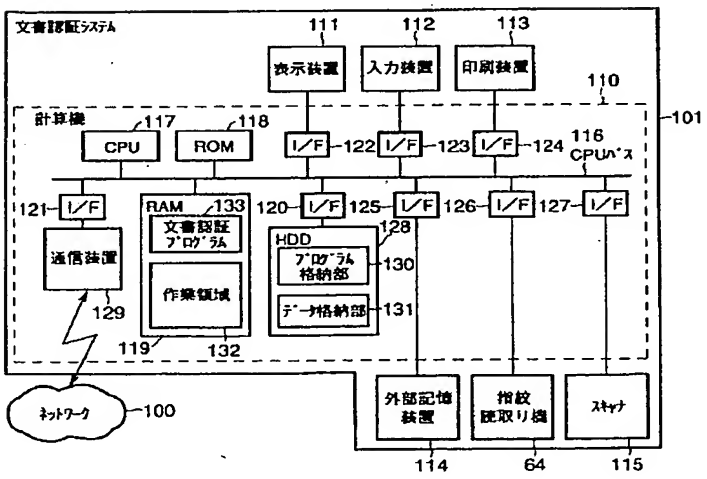
【図１】



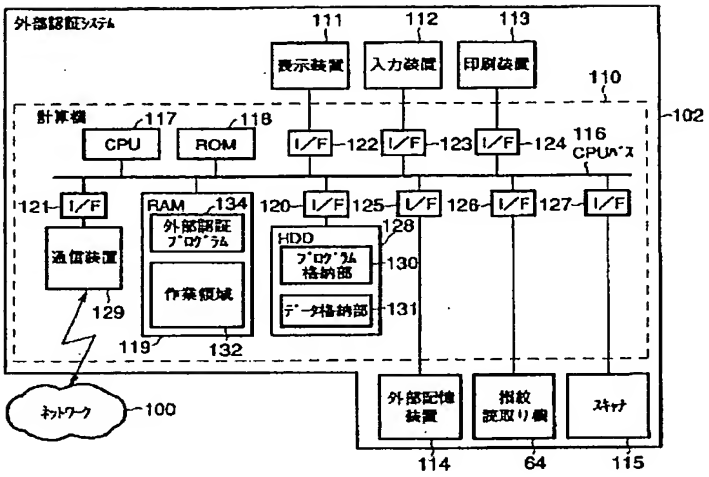
【図７】



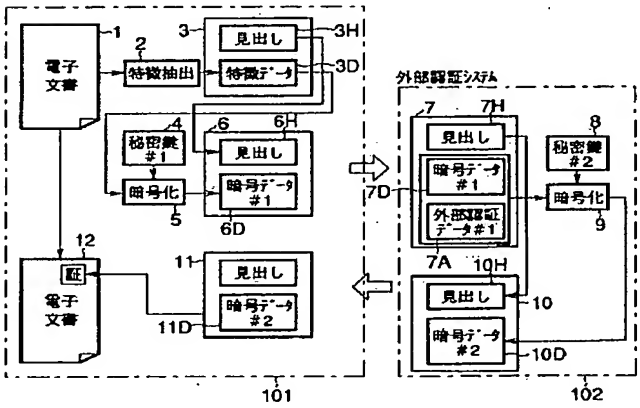
【図２】



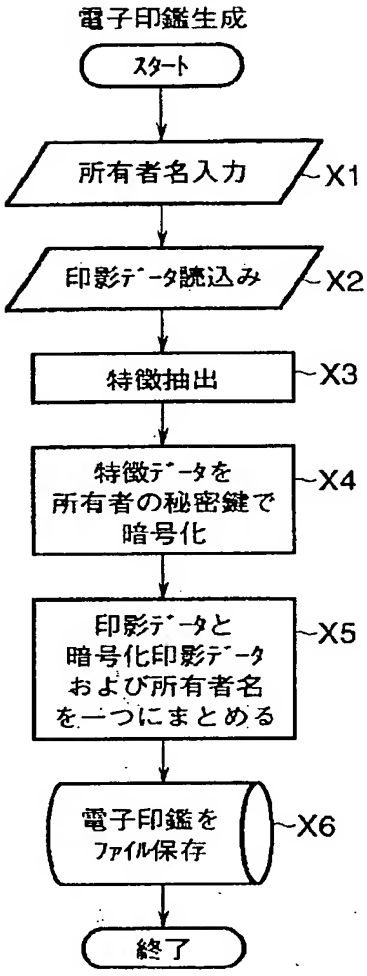
【図３】


外部認証システム
111
112
113
表示装置
入力装置
印刷装置
110
102
計算機
117
118
CPU
ROM
I/F
122
123
124
116
CPUバス
121
RAM
134
外部認証プログラム
作業領域
120
125
126
127
HDD
128
プログラム格納部
130
データ格納部
131
通信装置
129
119
132
ネットワーク
100
外部記憶装置
指紋読取り機
スキャナ
114
64
115

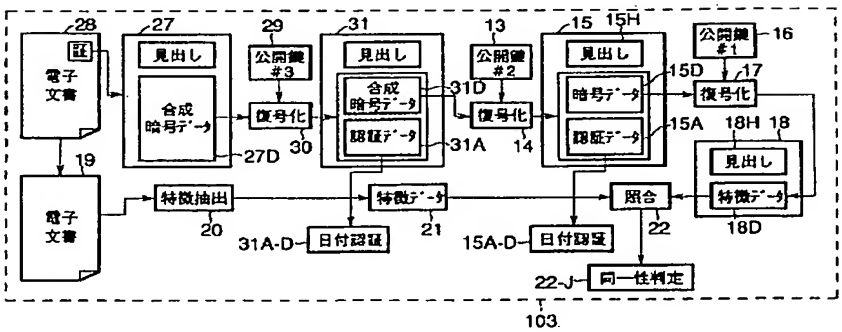
【図４】


電子文書
1
2
特徴抽出
3
見出し
特徴データ
3H
3D
秘密鍵#1
4
暗号化
5
6
6H
暗号データ#1
6D
12
証
11
暗号データ#2
11D
101
外部認証システム
7
7H
7D
7A
10H
10
10D
秘密鍵#2
8
9
外部認証データ#1
102

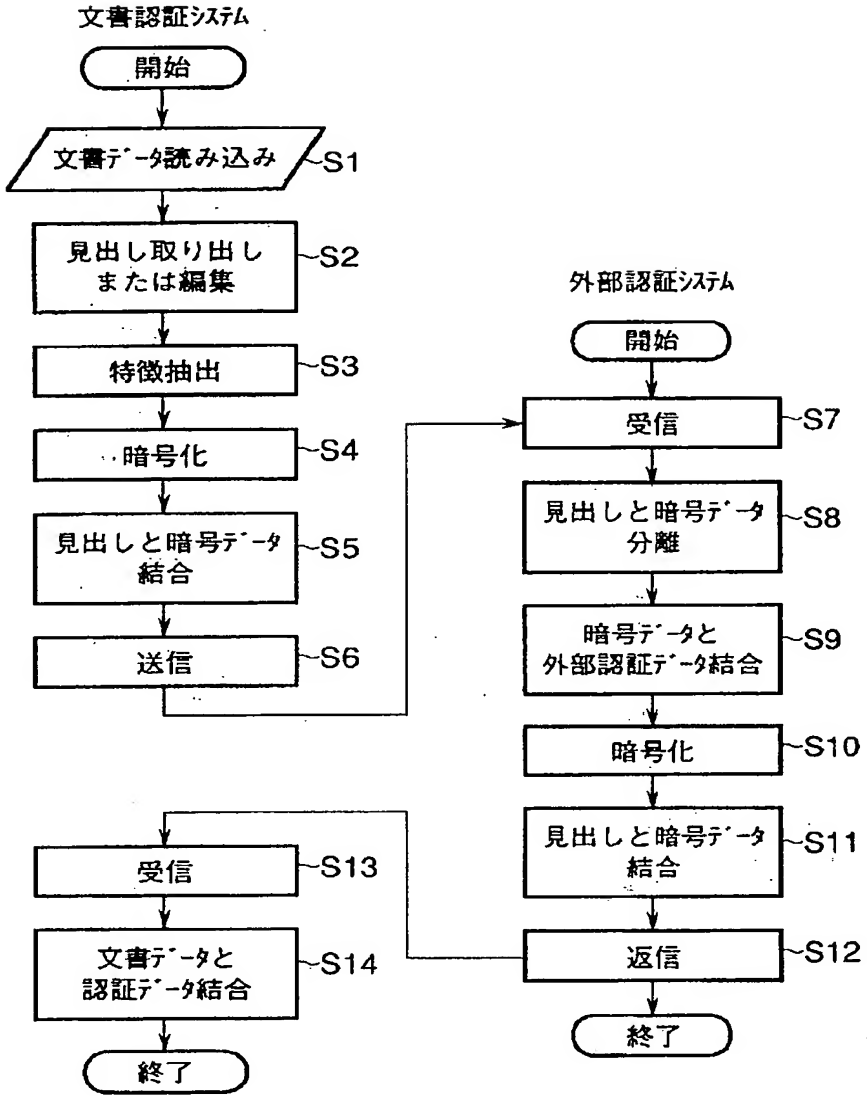
【図１７】


電子印鑑生成
スタート
所有者名入力
X1
印影データ読込み
X2
特徴抽出
X3
特徴データを所有者の秘密鍵で暗号化
X4
印影データと暗号化印影データおよび所有者名を一つにまとめる
X5
電子印鑑をファイル保存
X6
終了

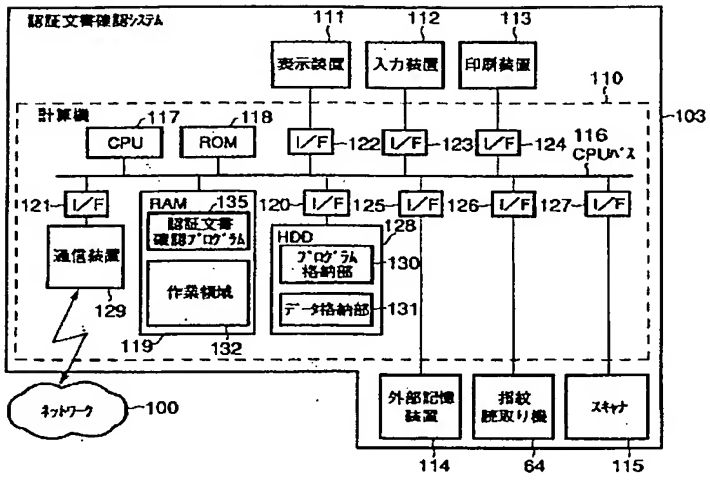
【図１１】


28
証
電子文書
19
27
見出し
合成暗号データ
27D
29
公開鍵#3
復号化
30
31
見出し
合成暗号データ
認証データ
31A
13
公開鍵#2
31D
復号化
14
15
15H
見出し
暗号データ
認証データ
15D
15A
公開鍵#1
16
17
復号化
18H
18
見出し
特徴データ
18D
特徴抽出
20
特徴データ
21
照合
22
31A-D
日付認証
15A-D
日付認証
22-J
同一性判定
103

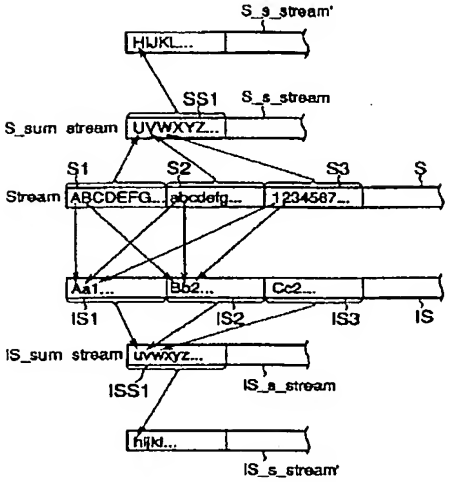
【図５】


文書認証システム
開始
文書データ読み込み
S1
見出し取り出しまたは編集
S2
特徴抽出
S3
暗号化
S4
見出しと暗号データ結合
S5
送信
S6
受信
S13
文書データと認証データ結合
S14
終了
外部認証システム
開始
受信
S7
見出しと暗号データ分離
S8
暗号データと外部認証データ結合
S9
暗号化
S10
見出しと暗号データ結合
S11
返信
S12
終了

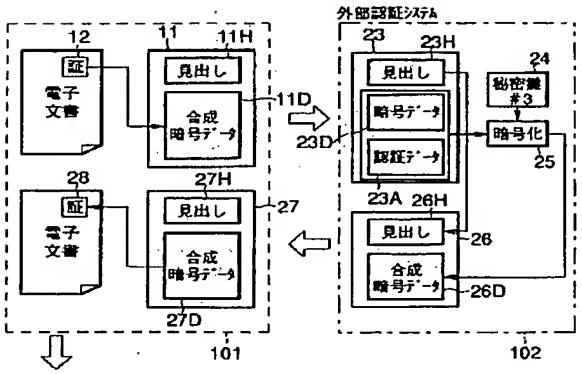
【図６】



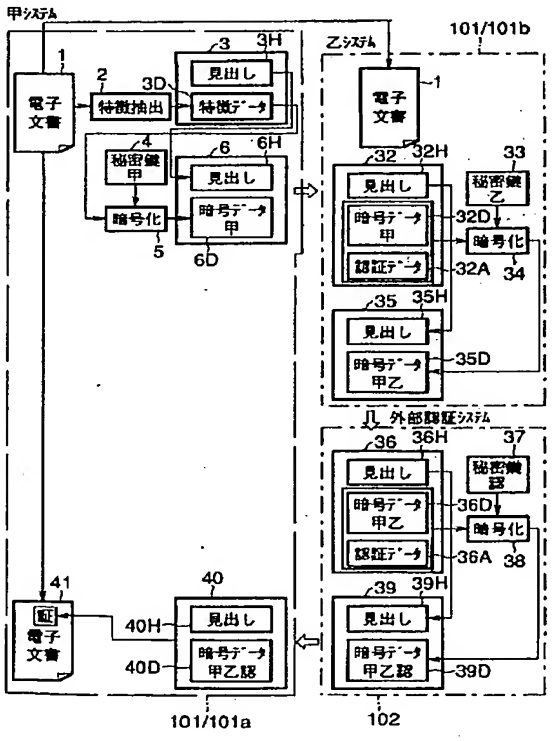
【図２３】



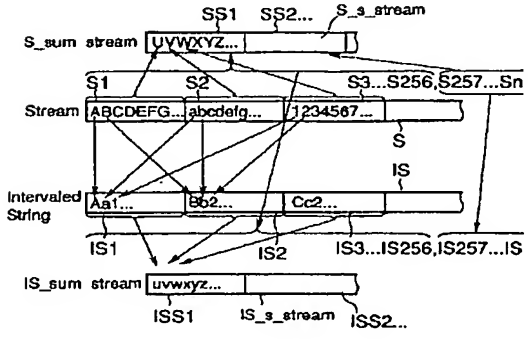
【図９】



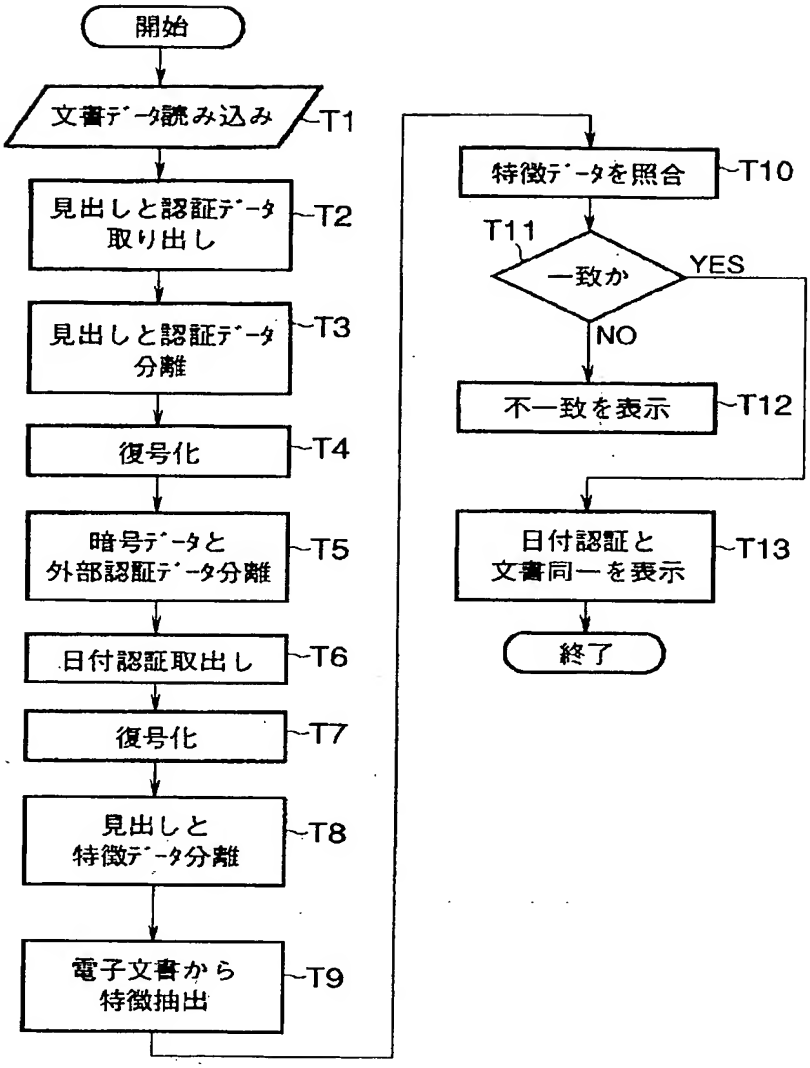
【図１３】



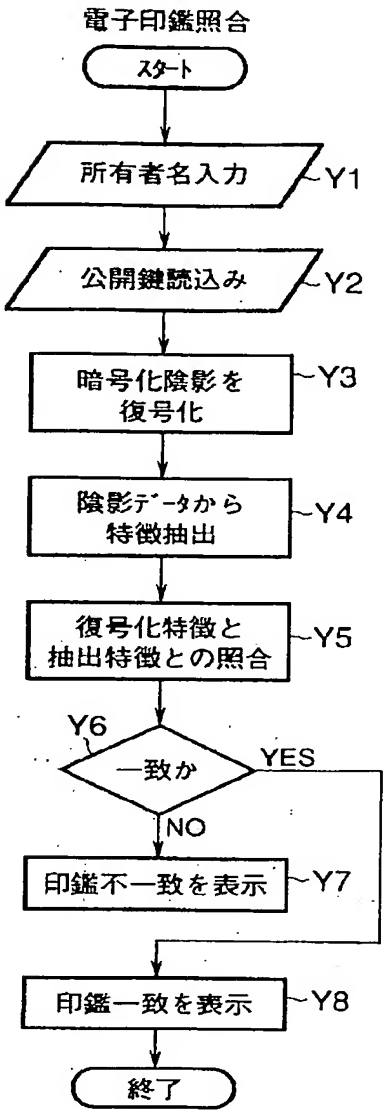
【図２０】



【図８】



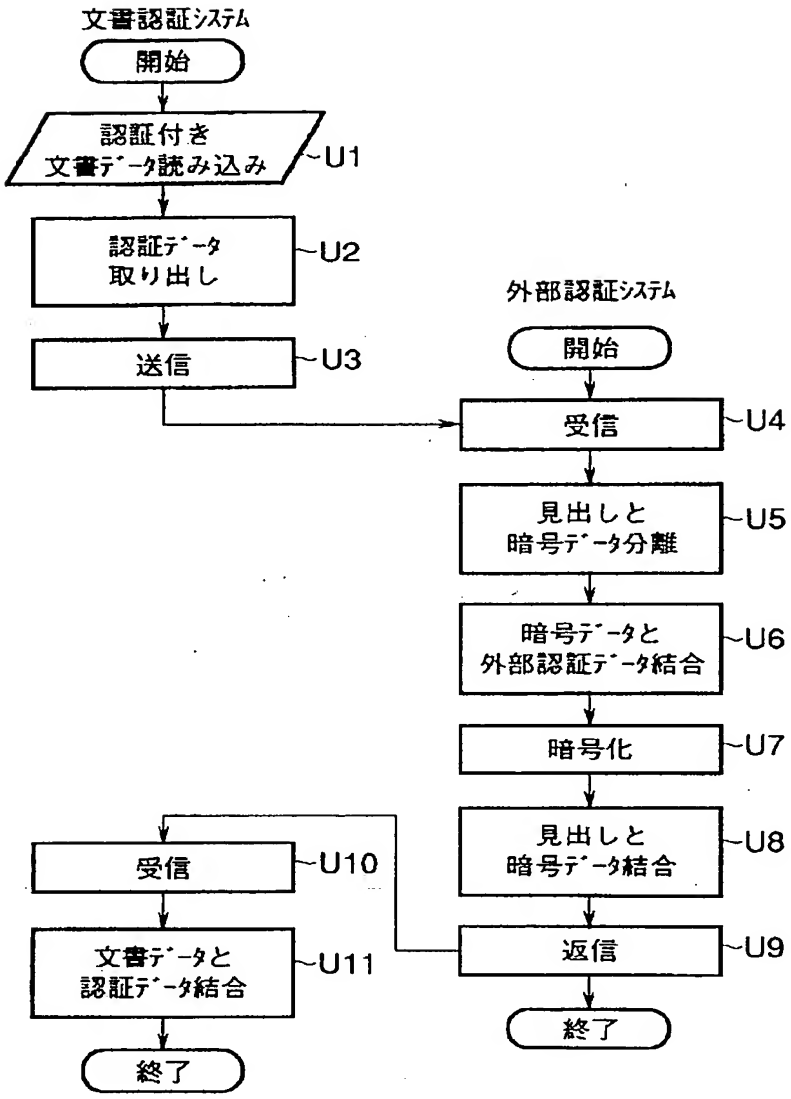
【図１８】



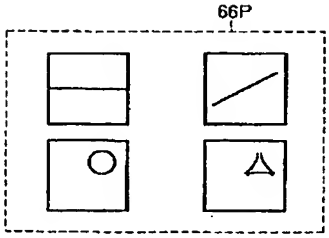
【図３２】

【図３３】

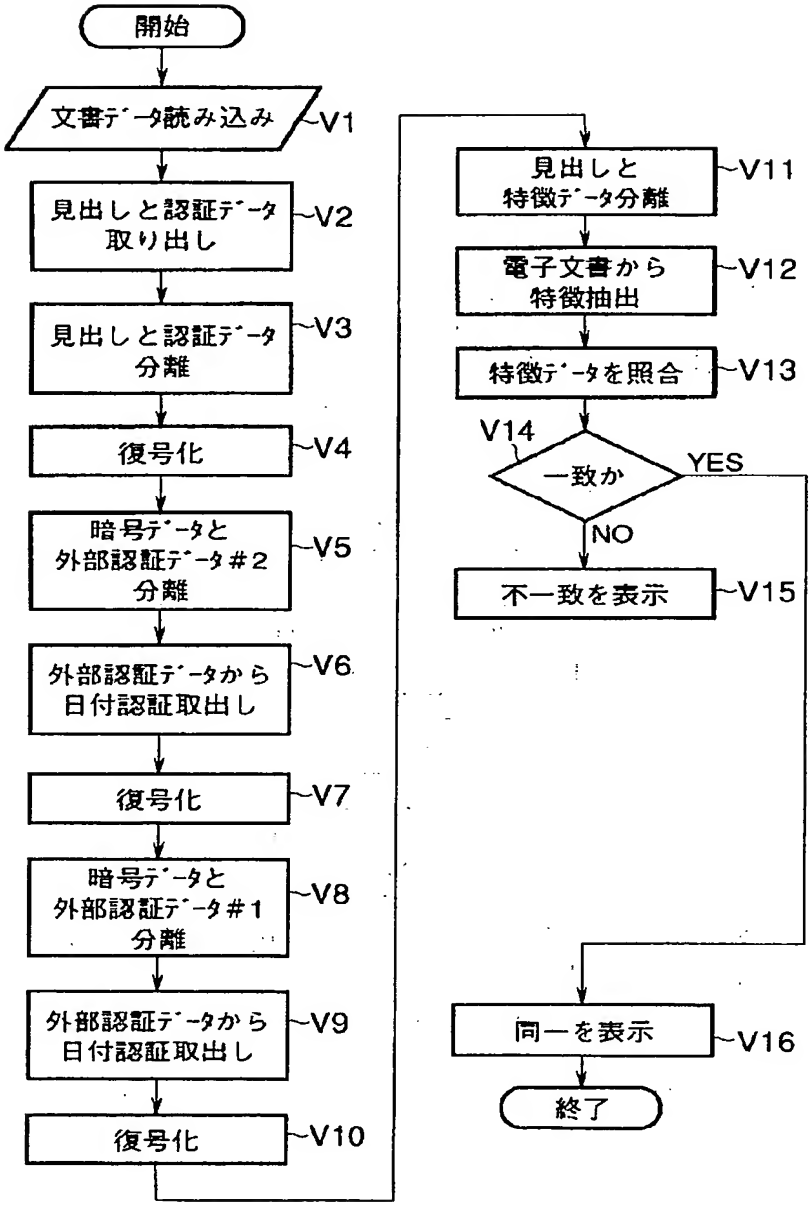
【図１０】


文書認証システム
開始
認証付き
文書データ読み込み
U1
認証データ
取り出し
U2
送信
U3
外部認証システム
開始
受信
U4
見出しと
暗号データ分離
U5
暗号データと
外部認証データ結合
U6
暗号化
U7
見出しと
暗号データ結合
U8
返信
U9
終了
受信
U10
文書データと
認証データ結合
U11
終了

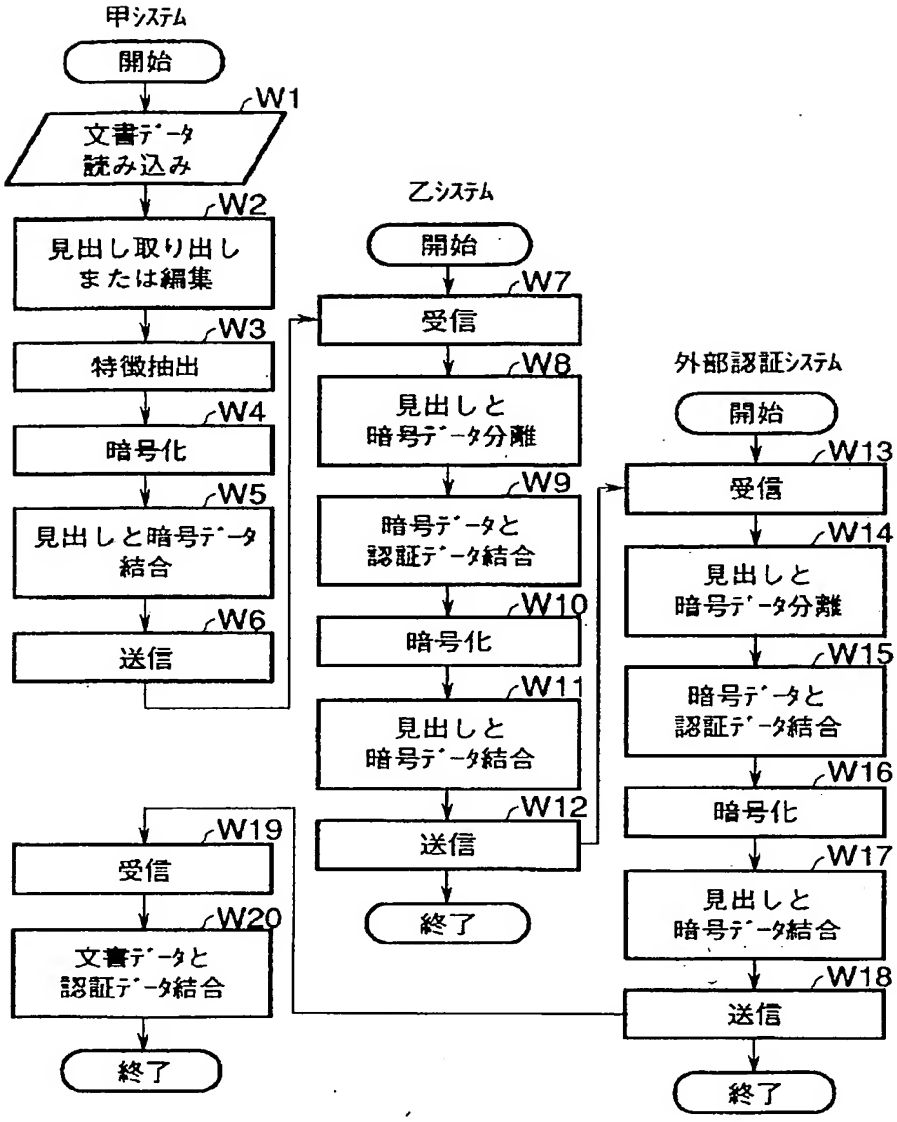
【図３４】


66P

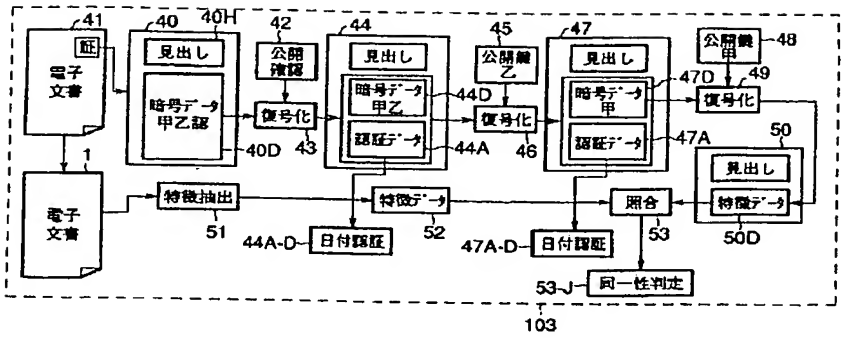
【図１２】


開始
文書ﾃﾞｰﾀ読み込み
V1
見出しと認証ﾃﾞｰﾀ取り出し
V2
見出しと認証ﾃﾞｰﾀ分離
V3
復号化
V4
暗号ﾃﾞｰﾀと外部認証ﾃﾞｰﾀ＃２分離
V5
外部認証ﾃﾞｰﾀから日付認証取出し
V6
復号化
V7
暗号ﾃﾞｰﾀと外部認証ﾃﾞｰﾀ＃１分離
V8
外部認証ﾃﾞｰﾀから日付認証取出し
V9
復号化
V10
見出しと特徴ﾃﾞｰﾀ分離
V11
電子文書から特徴抽出
V12
特徴ﾃﾞｰﾀを照合
V13
V14
一致か
YES
NO
不一致を表示
V15
同一を表示
V16
終了

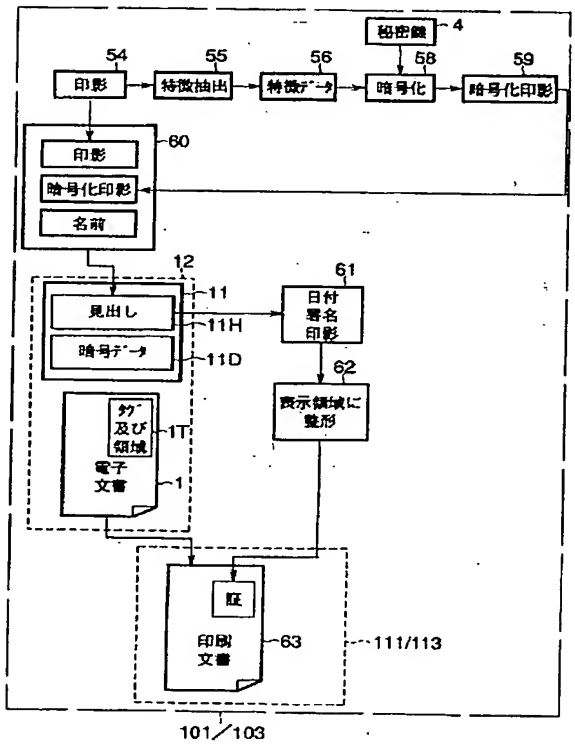
【図１４】


甲システム
開始
W1
文書データ
読み込み
W2
見出し取り出し
または編集
W3
特徴抽出
W4
暗号化
W5
見出しと暗号データ
結合
W6
送信
乙システム
開始
W7
受信
W8
見出しと
暗号データ分離
W9
暗号データと
認証データ結合
W10
暗号化
W11
見出しと
暗号データ結合
W12
送信
終了
外部認証システム
開始
W13
受信
W14
見出しと
暗号データ分離
W15
暗号データと
認証データ結合
W16
暗号化
W17
見出しと
暗号データ結合
W18
送信
終了
W19
受信
W20
文書データと
認証データ結合
終了

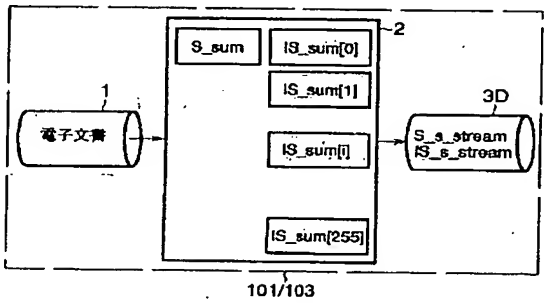
【図１５】



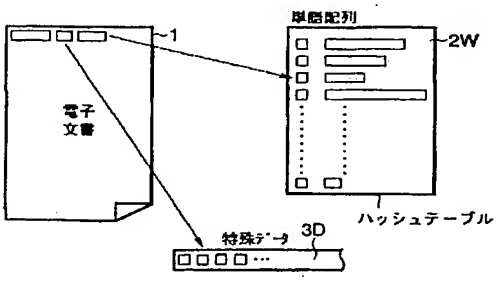
【図１６】



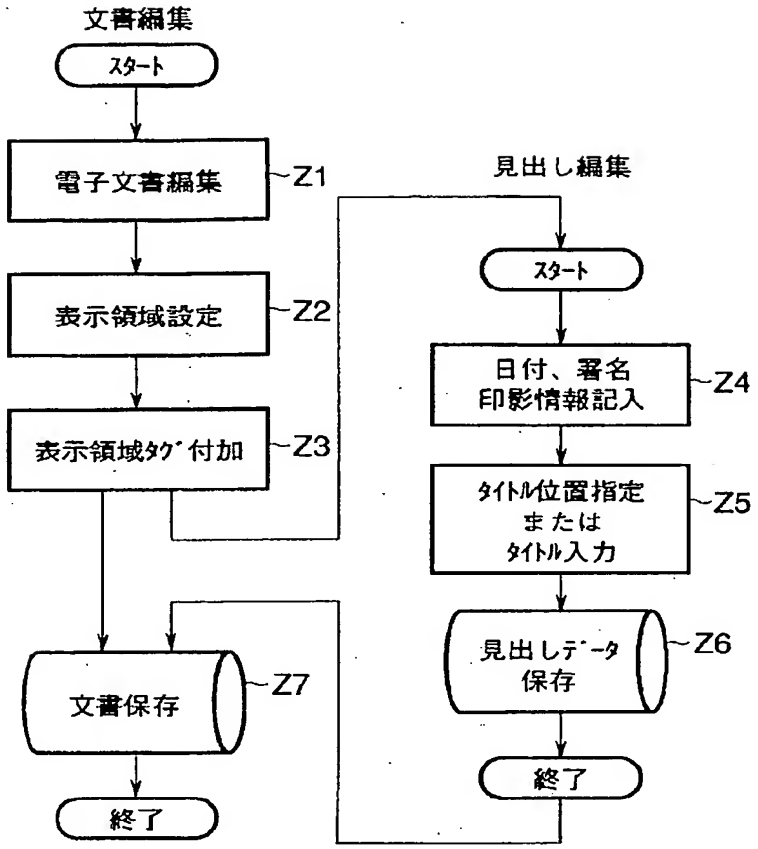
【図２１】



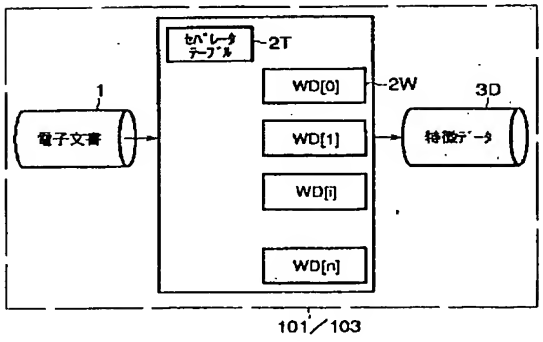
【図２４】



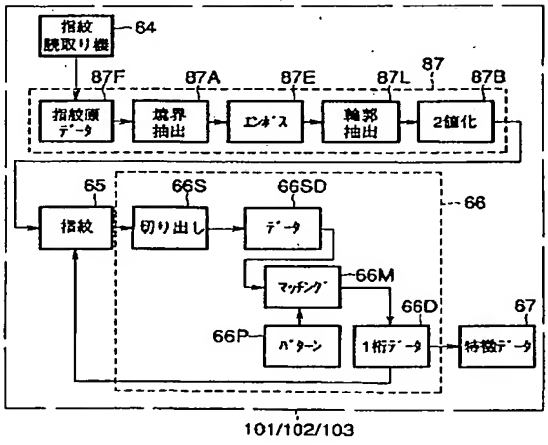
【図１９】


文書編集
スタート
電子文書編集
Z1
表示領域設定
Z2
表示領域ﾀｸﾞ付加
Z3
文書保存
Z7
終了
見出し編集
スタート
日付、署名
印影情報記入
Z4
ﾀｲﾄﾙ位置指定
または
ﾀｲﾄﾙ入力
Z5
見出しﾃﾞｰﾀ
保存
Z6
終了

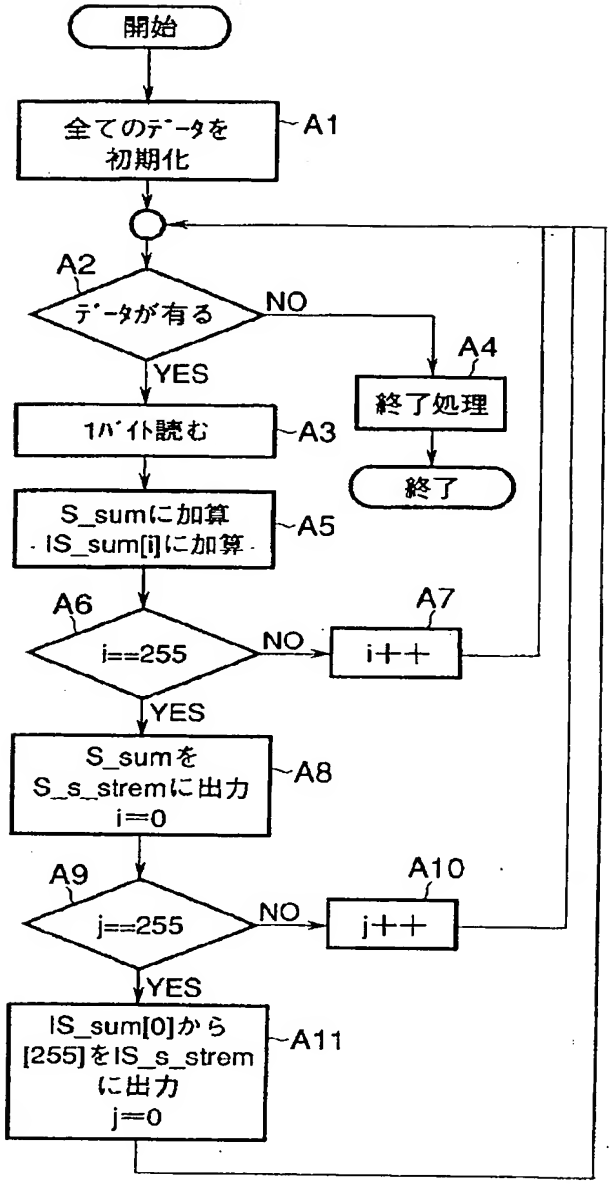
【図２５】


ｾﾊﾟﾚｰﾀ
ﾃｰﾌﾞﾙ
2T
WD[0]
WD[1]
WD[i]
WD[n]
2W
3D
1
電子文書
特徴ﾃﾞｰﾀ
101／103

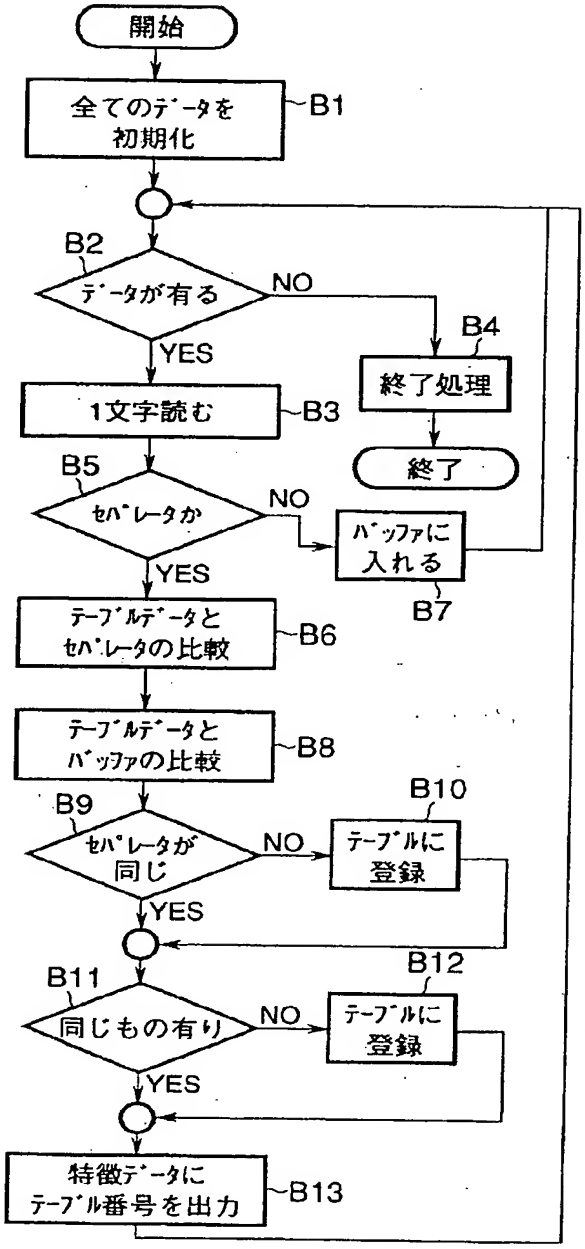
【図３１】


指紋
読取り機
64
87F
87A
87E
87L
87
87B
指紋原
ﾃﾞｰﾀ
境界
抽出
ｴｯｼﾞｽ
輪郭
抽出
2値化
65
66S
66SD
66
指紋
切り出し
ﾃﾞｰﾀ
ﾏｯﾁﾝｸﾞ
66M
66D
67
66P
ﾊﾟﾀｰﾝ
1桁ﾃﾞｰﾀ
特徴ﾃﾞｰﾀ
101/102/103

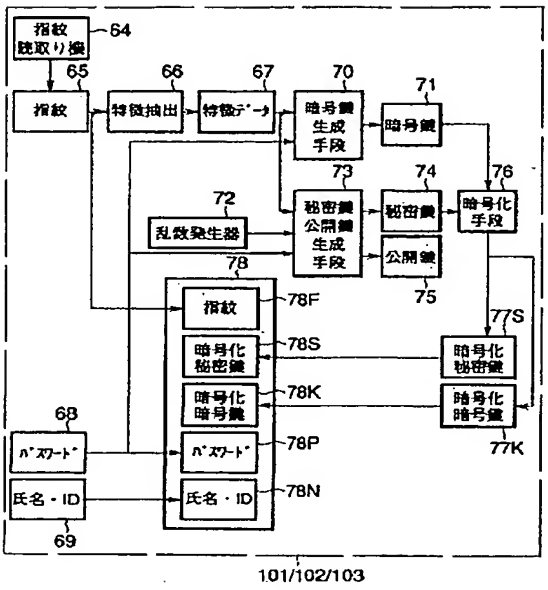
【図２２】


開始
全てのﾃﾞｰﾀを初期化
A1
A2
ﾃﾞｰﾀが有る
NO
YES
A4
終了処理
終了
1ﾊﾞｲﾄ読む
A3
S_sumに加算
IS_sum[i]に加算
A5
A6
i==255
NO
A7
i++
YES
S_sumを
S_s_stremに出力
i=0
A8
A9
j==255
NO
A10
j++
YES
IS_sum[0]から
[255]をIS_s_strem
に出力
j=0
A11

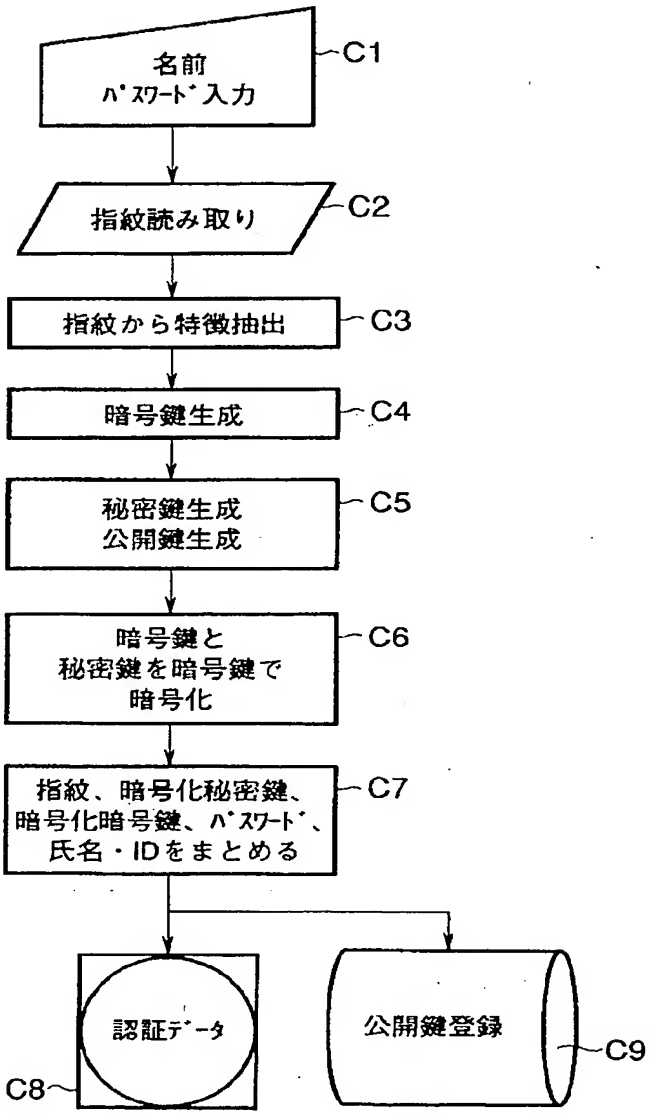
【図２６】


開始
全てのﾃﾞｰﾀを初期化
B1
B2
ﾃﾞｰﾀが有る
NO
YES
B4
終了処理
終了
1文字読む
B3
B5
ｾﾊﾟﾚｰﾀか
NO
ﾊﾞｯﾌｧに入れる
B7
YES
ﾃｰﾌﾞﾙﾃﾞｰﾀとｾﾊﾟﾚｰﾀの比較
B6
ﾃｰﾌﾞﾙﾃﾞｰﾀとﾊﾞｯﾌｧの比較
B8
B9
ｾﾊﾟﾚｰﾀが同じ
NO
B10
ﾃｰﾌﾞﾙに登録
YES
B11
同じもの有り
NO
B12
ﾃｰﾌﾞﾙに登録
YES
特徴ﾃﾞｰﾀにﾃｰﾌﾞﾙ番号を出力
B13

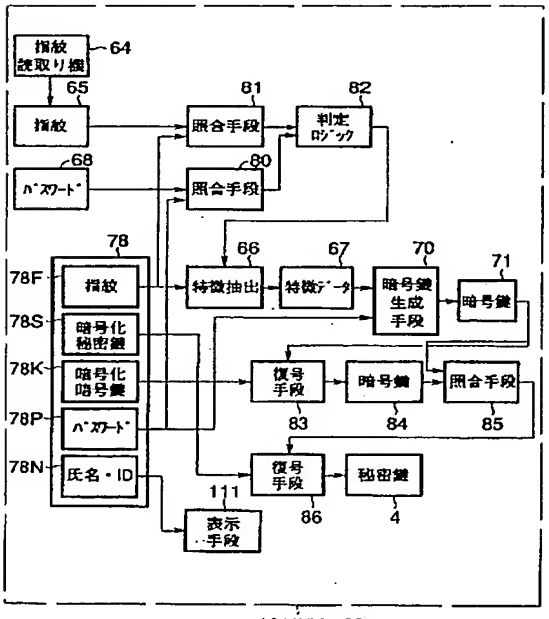
【図２７】


指紋読取り機
64
65
指紋
66
特徴抽出
67
特徴データ
70
暗号鍵生成手段
71
暗号鍵
72
乱数発生器
73
秘密鍵公開鍵生成手段
74
秘密鍵
75
公開鍵
76
暗号化手段
78
指紋
78F
暗号化秘密鍵
78S
暗号化暗号鍵
78K
パスワード
78P
氏名・ID
78N
77S
暗号化秘密鍵
暗号化暗号鍵
77K
68
パスワード
氏名・ID
69
101/102/103

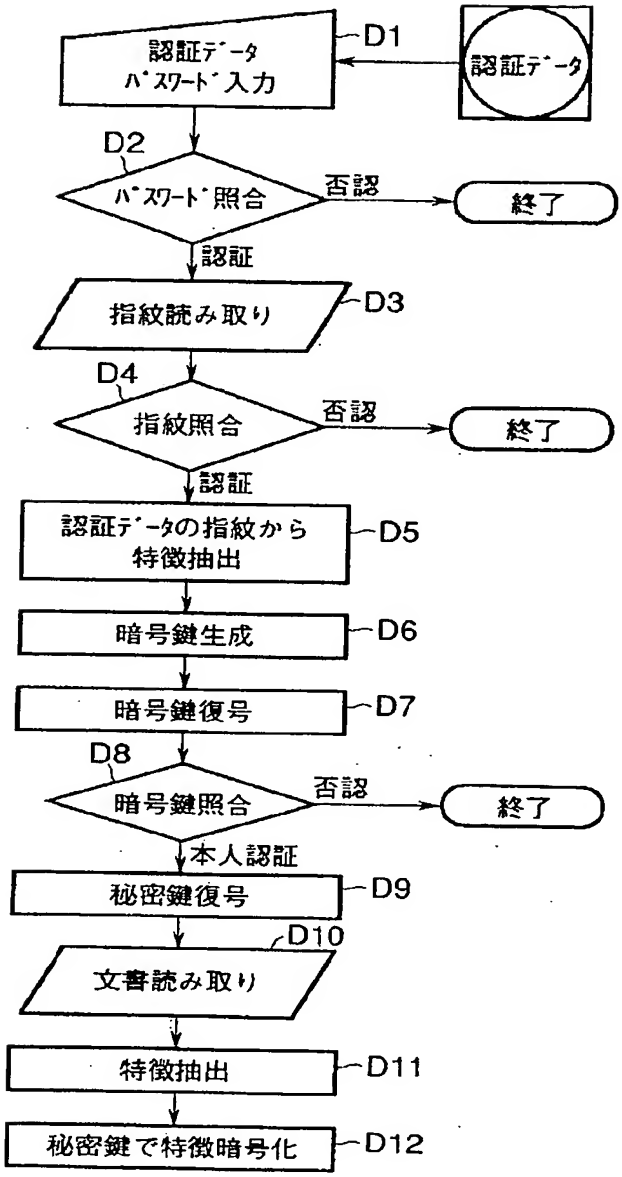
【図２８】


名前
パスワード入力
C1
指紋読み取り
C2
指紋から特徴抽出
C3
暗号鍵生成
C4
秘密鍵生成
公開鍵生成
C5
暗号鍵と
秘密鍵を暗号鍵で
暗号化
C6
指紋、暗号化秘密鍵、
暗号化暗号鍵、パスワード、
氏名・IDをまとめる
C7
認証データ
C8
公開鍵登録
C9

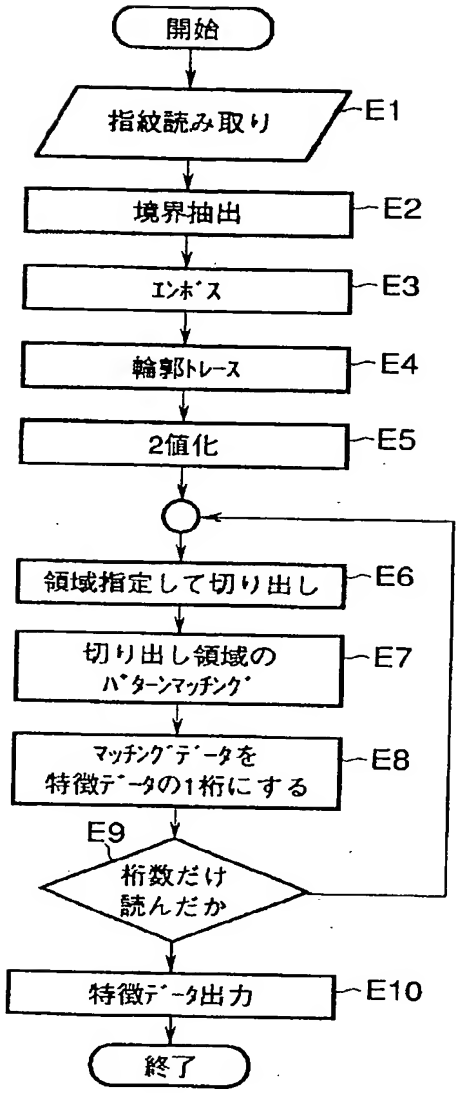
【図２９】


指紋読取り機
64
65
指紋
81
照合手段
82
判定ロジック
68
パスワード
80
照合手段
78
78F
指紋
78S
暗号化秘密鍵
78K
暗号化暗号鍵
78P
パスワード
78N
氏名・ID
66
特徴抽出
67
特徴データ
70
暗号鍵生成手段
71
暗号鍵
復号手段
83
暗号鍵
84
照合手段
85
復号手段
86
秘密鍵
4
111
表示手段
101/102/103

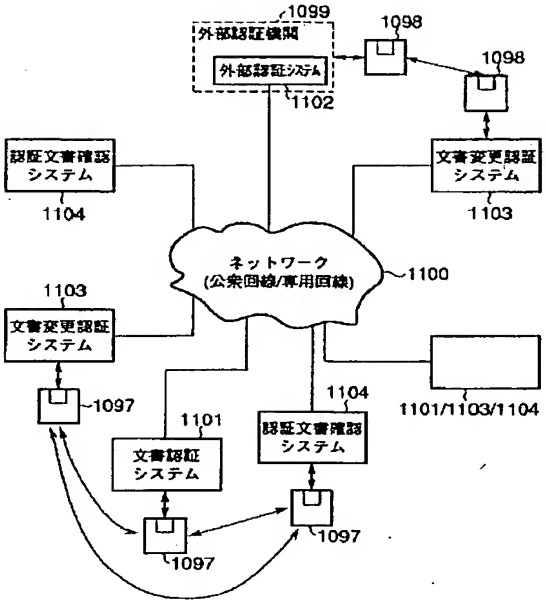
【図３０】


認証ﾃﾞｰﾀ
ﾊﾟｽﾜｰﾄﾞ入力
D1
認証ﾃﾞｰﾀ
D2
ﾊﾟｽﾜｰﾄﾞ照合
否認
終了
認証
指紋読み取り
D3
D4
指紋照合
否認
終了
認証
認証ﾃﾞｰﾀの指紋から
特徴抽出
D5
暗号鍵生成
D6
暗号鍵復号
D7
D8
暗号鍵照合
否認
終了
本人認証
秘密鍵復号
D9
D10
文書読み取り
特徴抽出
D11
秘密鍵で特徴暗号化
D12

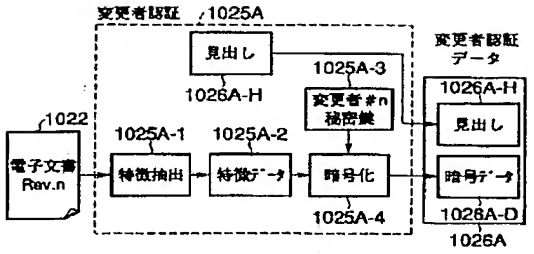
【図３５】


開始
指紋読み取り
E1
境界抽出
E2
ｴﾝﾎﾞｽ
E3
輪郭ﾄﾚｰｽ
E4
2値化
E5
領域指定して切り出し
E6
切り出し領域の
ﾊﾟﾀｰﾝﾏｯﾁﾝｸﾞ
E7
ﾏｯﾁﾝｸﾞﾃﾞｰﾀを
特徴ﾃﾞｰﾀの1桁にする
E8
E9
桁数だけ
読んだか
特徴ﾃﾞｰﾀ出力
E10
終了

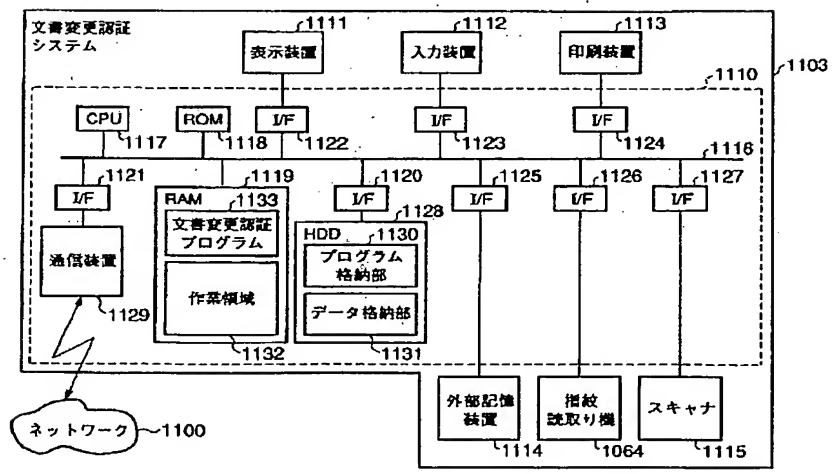
【図３６】


外部認証機関
外部認証システム
1102
1099
1098
1098
認証文書確認システム
1104
文書変更認証システム
1103
ネットワーク
(公衆回線/専用回線)
1100
1103
文書変更認証システム
1097
1101
文書認証システム
1104
認証文書確認システム
1097
1097
1101/1103/1104

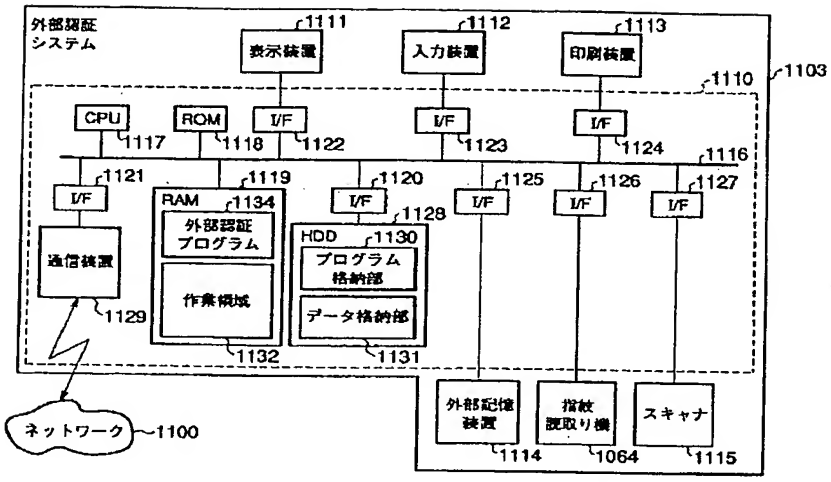
【図４１】


変更者認証
1025A
見出し
1026A-H
1025A-3
変更者#n秘密鍵
1022
電子文書 Rev.n
1025A-1
特徴抽出
1025A-2
特徴データ
暗号化
1025A-4
変更者認証データ
1026A-H
見出し
暗号データ
1026A-D
1026A

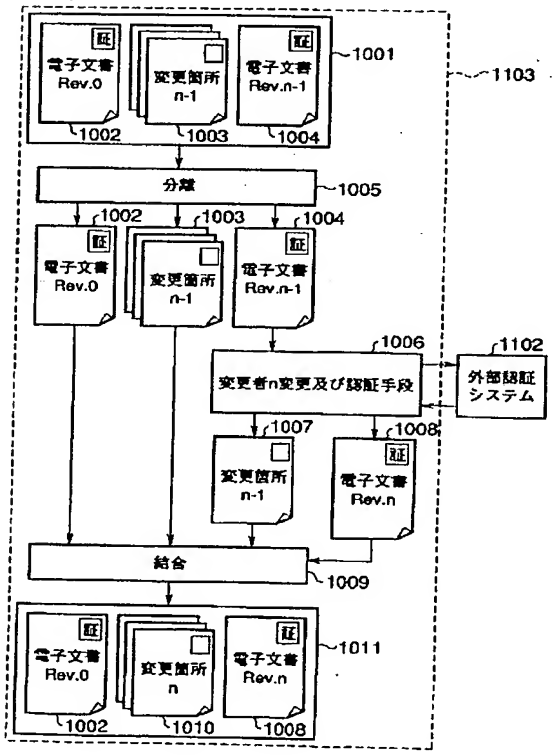
【図３７】


文書変更認証システム
1111
表示装置
1112
入力装置
1113
印刷装置
1110
1103
CPU
1117
ROM
1118
I/F
1122
I/F
1123
I/F
1124
1116
1121
I/F
1119
RAM
1133
文書変更認証プログラム
作業領域
1132
1120
I/F
1128
HDD
1130
プログラム格納部
データ格納部
1131
1125
I/F
1126
I/F
1127
I/F
通信装置
1129
外部記憶装置
1114
指紋読取り機
1064
スキャナ
1115
ネットワーク
1100

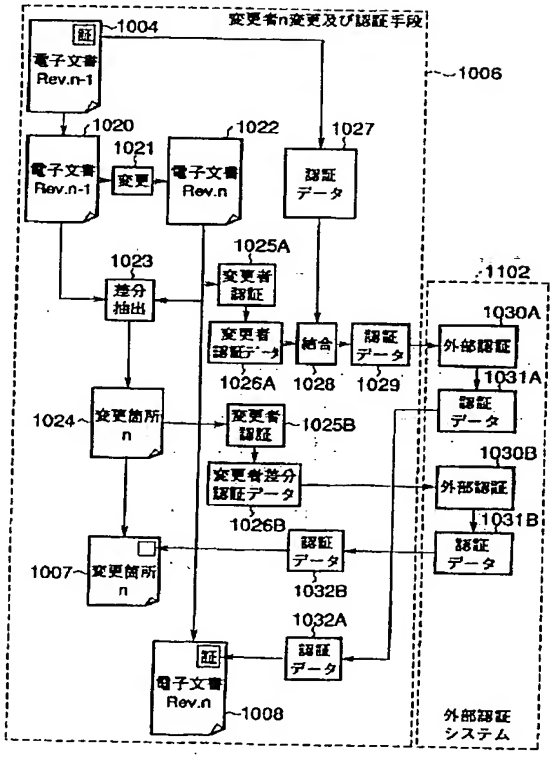
【図３８】


外部認証システム
1111
表示装置
1112
入力装置
1113
印刷装置
1110
1103
CPU
1117
ROM
1118
I/F
1122
I/F
1123
I/F
1124
1116
I/F
1121
RAM
1134
外部認証プログラム
作業領域
1119
I/F
1120
1128
I/F
1125
I/F
1126
I/F
1127
HDD
1130
プログラム格納部
データ格納部
1131
通信装置
1129
1132
ネットワーク
1100
外部記憶装置
1114
指紋読取り機
1064
スキャナ
1115

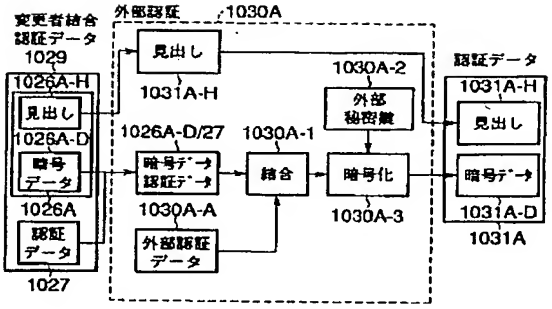
【図３９】


電子文書 Rev.0
1002
変更箇所 n-1
1003
電子文書 Rev.n-1
1004
1001
1103
分離
1005
1006
変更者n変更及び認証手段
1102
外部認証システム
変更箇所 n-1
1007
電子文書 Rev.n
1008
結合
1009
変更箇所 n
1010
1011

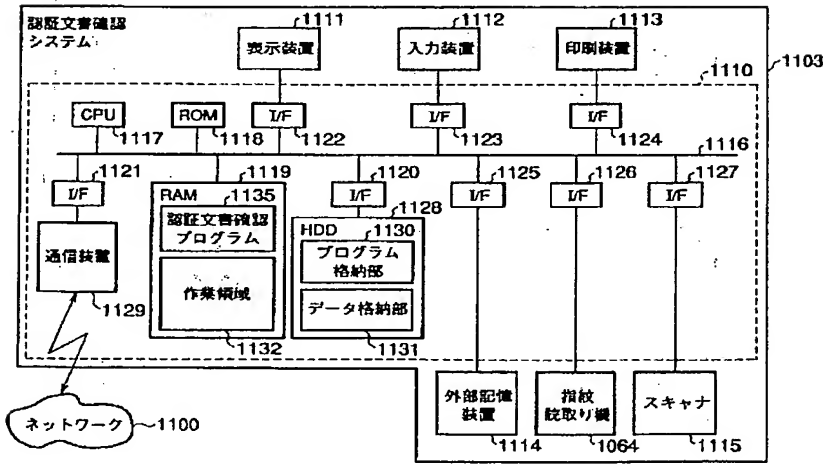
【図４０】


変更者n変更及び認証手段
1004
電子文書 Rev.n-1
1006
1020
1021
変更
1022
電子文書 Rev.n
1027
認証データ
1023
差分抽出
1025A
変更者認証
1102
変更者認証データ
1026A
結合
1028
認証データ
1029
1030A
外部認証
1031A
認証データ
1024
変更箇所 n
変更者認証
1025B
1030B
外部認証
変更者差分認証データ
1026B
1031B
認証データ
1007
変更箇所 n
認証データ
1032B
1032A
認証データ
電子文書 Rev.n
1008
外部認証システム

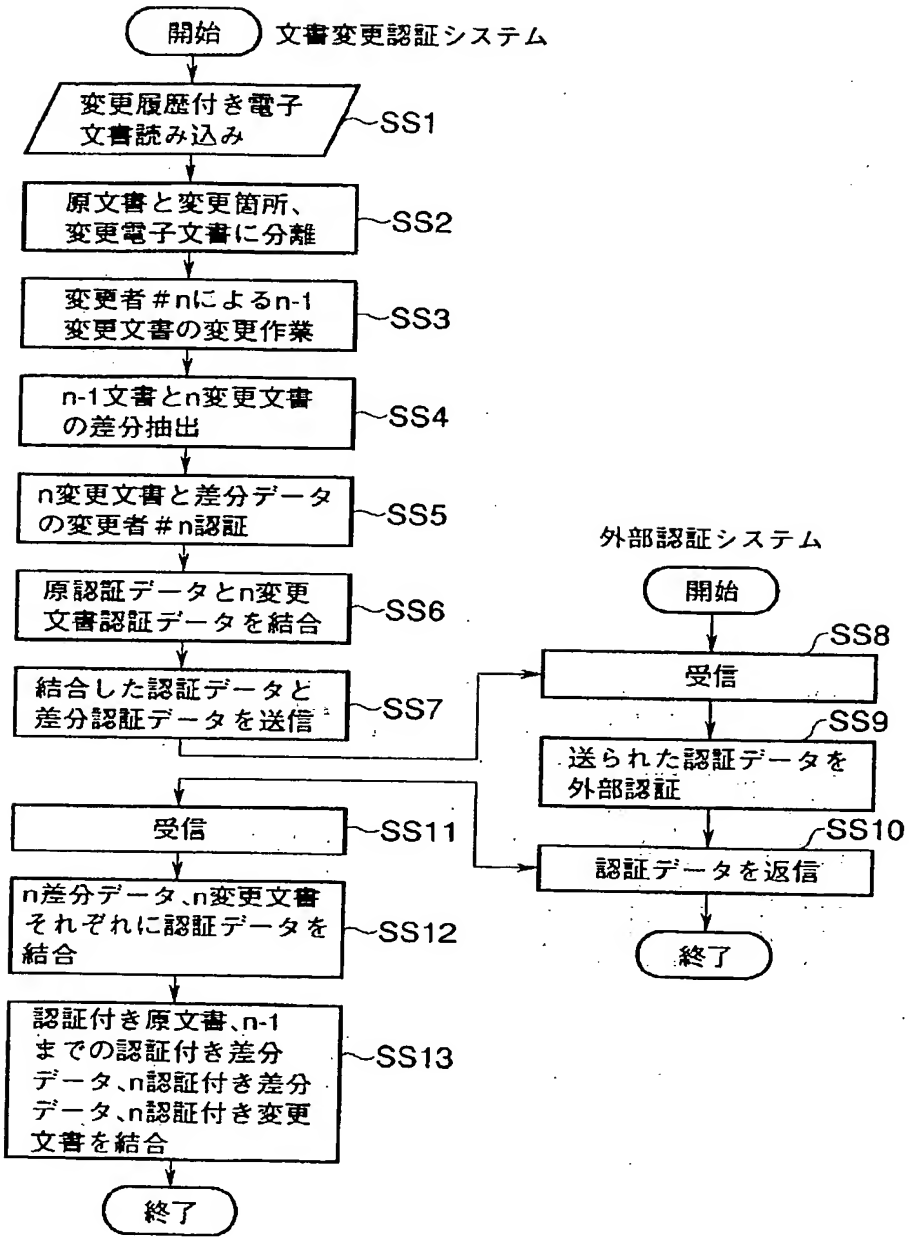
【図４２】


変更者結合
認証データ
1029
1026A-H
見出し
1026A-D
暗号
データ
1026A
認証
データ
1027
外部認証
1030A
見出し
1031A-H
1026A-D/27
暗号データ
認証データ
1030A-A
外部認証
データ
1030A-1
結合
1030A-2
外部
秘密鍵
暗号化
1030A-3
認証データ
1031A-H
見出し
暗号データ
1031A-D
1031A

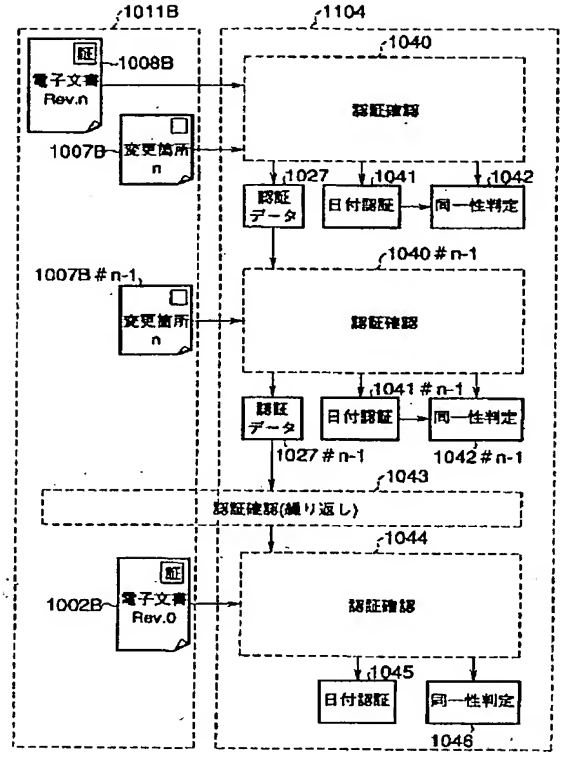
【図４４】


認証文書確認
システム
1111
表示装置
1112
入力装置
1113
印刷装置
1110
1103
CPU
1117
ROM
1118
I/F
1122
I/F
1123
I/F
1124
1116
1121
1119
1120
1125
1126
1127
I/F
RAM
1135
認証文書確認
プログラム
作業領域
1132
I/F
1128
HDD
1130
プログラム
格納部
データ格納部
1131
I/F
I/F
I/F
通信装置
1129
ネットワーク
1100
外部記憶
装置
1114
指紋
読取り機
1064
スキャナ
1115

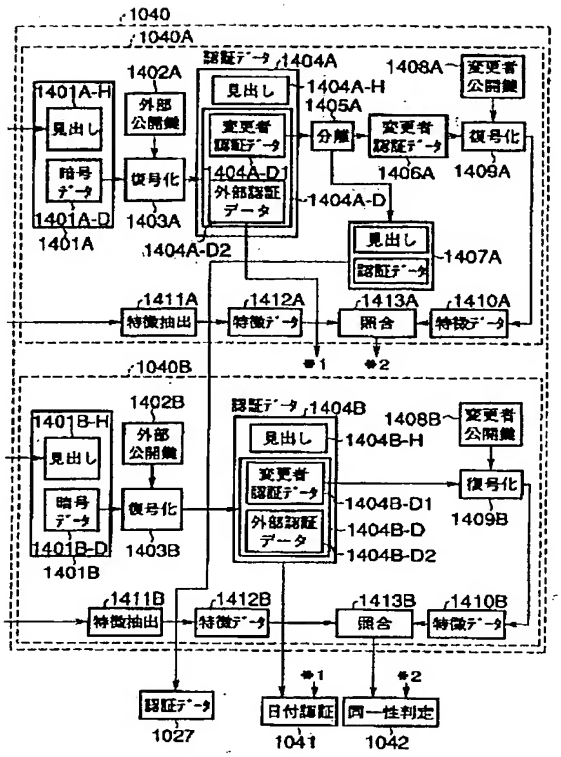
【図４３】


開始
文書変更認証システム
変更履歴付き電子文書読み込み
SS1
原文書と変更箇所、変更電子文書に分離
SS2
変更者＃nによるn-1変更文書の変更作業
SS3
n-1文書とn変更文書の差分抽出
SS4
n変更文書と差分データの変更者＃n認証
SS5
原認証データとn変更文書認証データを結合
SS6
結合した認証データと差分認証データを送信
SS7
外部認証システム
開始
受信
SS8
送られた認証データを外部認証
SS9
認証データを返信
SS10
終了
受信
SS11
n差分データ、n変更文書それぞれに認証データを結合
SS12
認証付き原文書、n-1までの認証付き差分データ、n認証付き差分データ、n認証付き変更文書を結合
SS13
終了

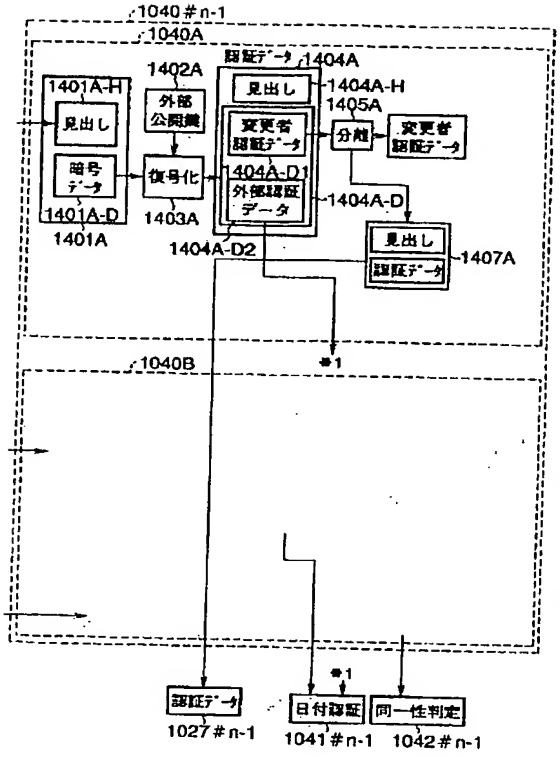
【図４５】


1011B
1104
1040
認証
電子文書
Rev.n
1008B
1007B
変更箇所
n
認証確認
1027
1041
1042
認証
データ
日付認証
同一性判定
1040＃n-1
1007B＃n-1
変更箇所
n
認証確認
1041＃n-1
認証
データ
日付認証
同一性判定
1027＃n-1
1042＃n-1
1043
認証確認(繰り返し)
1044
1002B
認証
電子文書
Rev.0
認証確認
1045
日付認証
同一性判定
1046

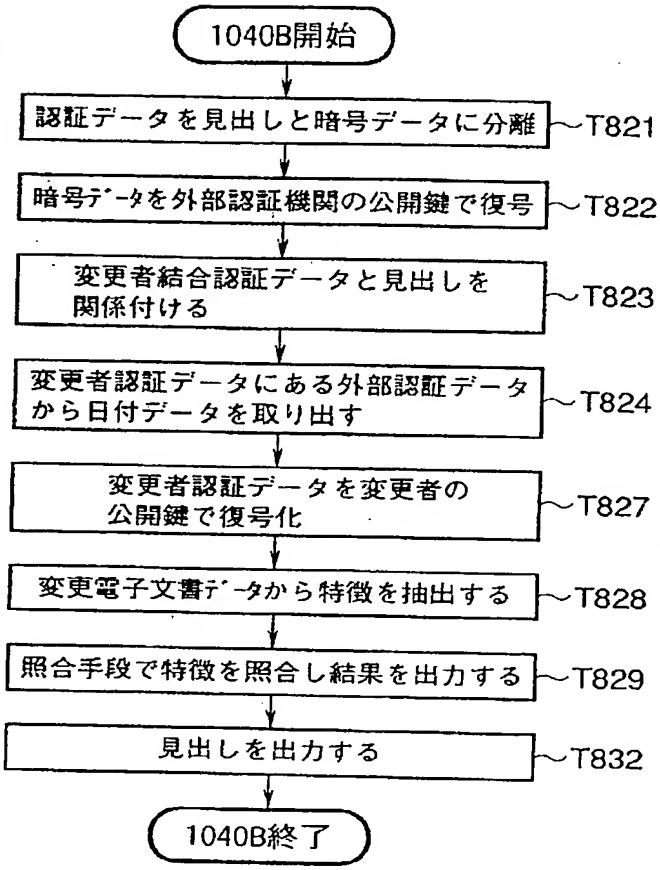
【図４６】


1040
1040A
認証データ
1404A
1408A
変更者
公開鍵
1401A-H
見出し
1402A
外部
公開鍵
見出し
1404A-H
1405A
分離
変更者
認証データ
復号化
1409A
暗号
データ
復号化
1404A-D1
外部認証
データ
1404A-D
1406A
1401A-D
1401A
1403A
1404A-D2
見出し
認証データ
1407A
1411A
特徴抽出
1412A
特徴データ
1413A
照合
1410A
特徴データ
＊1
＊2
1040B
1401B-H
見出し
1402B
外部
公開鍵
認証データ
1404B
1408B
変更者
公開鍵
見出し
1404B-H
変更者
認証データ
復号化
1409B
暗号
データ
復号化
1404B-D1
外部認証
データ
1404B-D
1404B-D2
1401B-D
1401B
1403B
1411B
特徴抽出
1412B
特徴データ
1413B
照合
1410B
特徴データ
＊1
＊2
認証データ
1027
日付認証
1041
同一性判定
1042

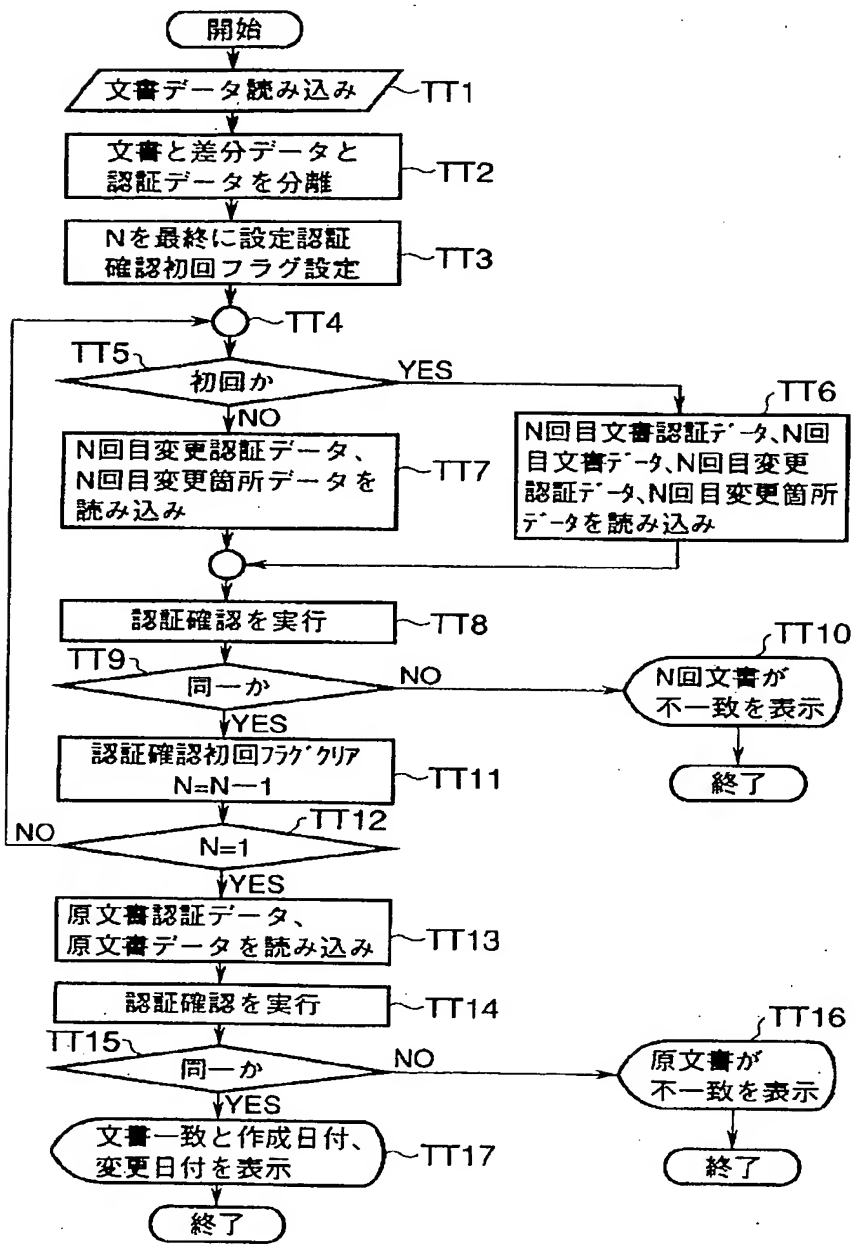
【図４７】


1040#n-1
1040A
1402A
認証ﾃﾞｰﾀ
1404A
1401A-H
見出し
外部公開鍵
1404A-H
1405A
変更者認証ﾃﾞｰﾀ
分離
変更者認証ﾃﾞｰﾀ
暗号ﾃﾞｰﾀ
復号化
1404A-D1
外部認証データ
1404A-D
1401A-D
1401A
1403A
1404A-D2
見出し
認証ﾃﾞｰﾀ
1407A
1040B
*1
*1
認証ﾃﾞｰﾀ
日付認証
同一性判定
1027#n-1
1041#n-1
1042#n-1

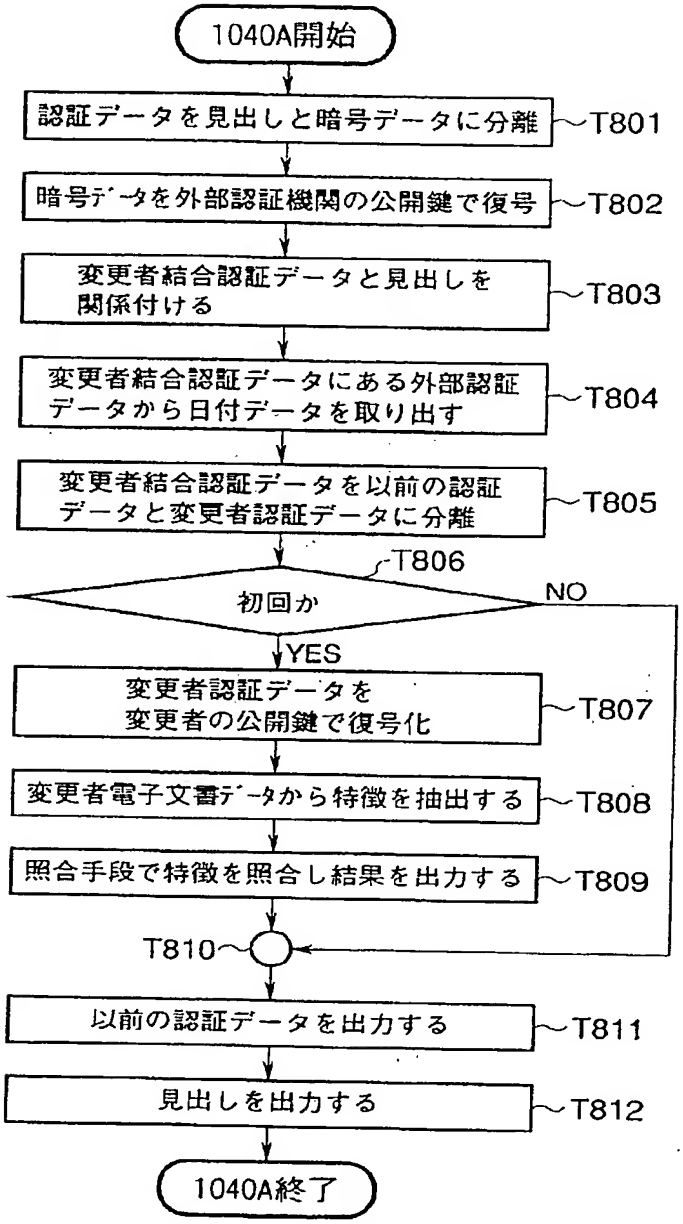
【図５０】


1040B開始
認証データを見出しと暗号データに分離
T821
暗号ﾃﾞｰﾀを外部認証機関の公開鍵で復号
T822
変更者結合認証データと見出しを関係付ける
T823
変更者認証データにある外部認証データから日付データを取り出す
T824
変更者認証データを変更者の公開鍵で復号化
T827
変更電子文書ﾃﾞｰﾀから特徴を抽出する
T828
照合手段で特徴を照合し結果を出力する
T829
見出しを出力する
T832
1040B終了

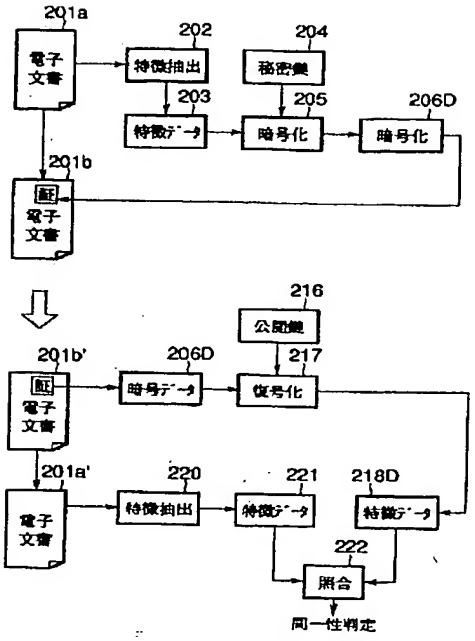
【図４８】


開始
文書データ読み込み
TT1
文書と差分データと認証データを分離
TT2
Nを最終に設定認証確認初回フラグ設定
TT3
TT4
TT5
初回か
YES
NO
TT6
N回目文書認証ﾃﾞｰﾀ、N回目文書ﾃﾞｰﾀ、N回目変更認証ﾃﾞｰﾀ、N回目変更箇所ﾃﾞｰﾀを読み込み
N回目変更認証データ、N回目変更箇所データを読み込み
TT7
認証確認を実行
TT8
TT9
同一か
NO
TT10
N回文書が不一致を表示
終了
YES
認証確認初回ﾌﾗｸﾞｸﾘｱ N=N−1
TT11
TT12
N=1
NO
YES
原文書認証データ、原文書データを読み込み
TT13
認証確認を実行
TT14
TT15
同一か
NO
TT16
原文書が不一致を表示
終了
YES
文書一致と作成日付、変更日付を表示
TT17
終了

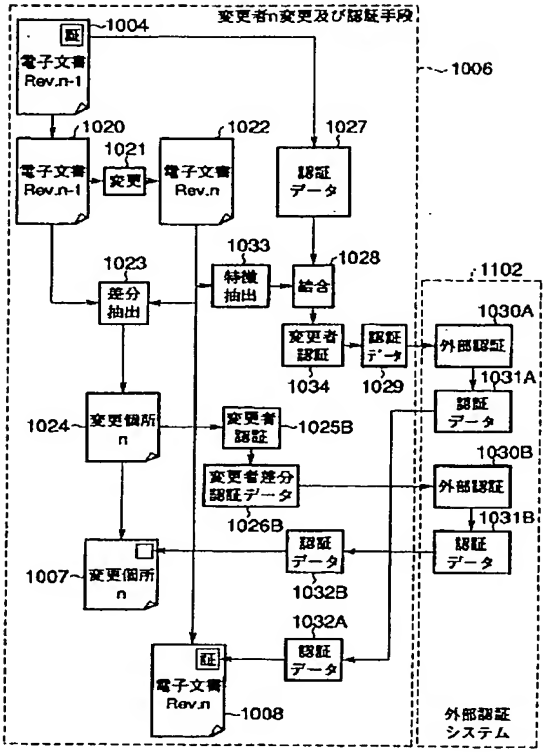
【図４９】


1040A開始
認証データを見出しと暗号データに分離
T801
暗号データを外部認証機関の公開鍵で復号
T802
変更者結合認証データと見出しを関係付ける
T803
変更者結合認証データにある外部認証データから日付データを取り出す
T804
変更者結合認証データを以前の認証データと変更者認証データに分離
T805
T806
初回か
NO
YES
変更者認証データを変更者の公開鍵で復号化
T807
変更者電子文書データから特徴を抽出する
T808
照合手段で特徴を照合し結果を出力する
T809
T810
以前の認証データを出力する
T811
見出しを出力する
T812
1040A終了

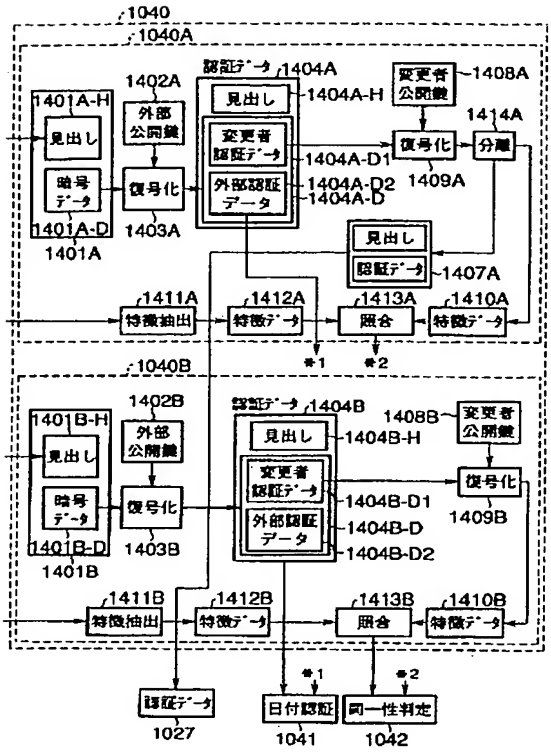
【図５３】


201a
電子文書
202
特徴抽出
204
秘密鍵
203
特徴データ
205
暗号化
206D
暗号化
201b
証
電子文書
216
公開鍵
201b'
206D
217
証
電子文書
暗号データ
復号化
201a'
220
221
218D
電子文書
特徴抽出
特徴データ
特徴データ
222
照合
同一性判定

【図５１】



【図５２】



フロントページの続き

(51)Int.Cl.[6]	識別記号	FI
		H04L 9/00　675D